OLYMPIC COUNCIL OF ASIA

Olympic Council of Asia (OCA) Organizational Structure & Policies and Procedures Handbook

Aug 2025
Ver 2.0

Table of Content

Introduction

Welcome to the Policies and Procedures Handbook of the Olympic Council of Asia (OCA). This comprehensive guide is designed to provide a structured framework outlining the essential policies and procedures governing the operations, conduct, and standards within our esteemed organization.

Purpose and Significance:

At the heart of the OCA's operations lie the principles of integrity, fairness, and excellence. This handbook serves as a testament to our commitment to upholding these values by establishing clear and comprehensive policies and procedures. These guidelines are essential in ensuring consistent and ethical practices across all facets of our organization's functions, from governance to operational execution.

Alignment with OCA's Mission:

Aligned with the OCA's mission to promote and develop sport, culture, and education in Asia, these policies and procedures aim to foster an environment conducive to the growth of athletics, regional cooperation, and organizational excellence. By adhering to these standards, we reinforce our dedication to transparency, accountability, and inclusivity, thereby enhancing the reputation and effectiveness of the OCA within the global sporting community.

Framework and Structure:

This handbook is structured to provide a clear understanding of our organizational policies and procedures. Each section is meticulously crafted to address specific aspects of our operations, including but not limited to governance, ethics, security, compliance, and operational protocols.

Commitment to Continuous Improvement:

As an organization committed to continuous improvement, this handbook is a living document subject to periodic reviews and updates. Our commitment to staying abreast of evolving best practices, regulatory changes, and technological advancements ensures that these policies and procedures remain relevant, effective, and aligned with the OCA's evolving goals and industry standards.

Utilization and Accessibility:

The Policies and Procedures Handbook is a vital resource for all individuals associated with the OCA, including board members, executives, staff, athletes, partners, and stakeholders. It is easily accessible to guide decision-making, operational activities, training, and adherence to the established norms.

Conclusion:

We encourage all members of the OCA community to familiarize themselves with this handbook and actively apply its guidelines in their respective roles. By collectively upholding these policies and procedures, we reaffirm our commitment to the highest standards of excellence, integrity, and success in the pursuit of our shared goals.

Message from the CEO/ Director General

The policies and procedures manual across all departments of the Olympic Council of Asia (OCA) is developed based on the fundamental principles outlined in the OCA Constitution and decisions ratified by the OCA Executive Board (EB) and relevant committees. This comprehensive manual aims to establish consistent and structured guidelines that align with the core values and objectives of the OCA, fostering operational efficiency and integrity.

Its overarching objective is to ensure that all departments maintain standardized practices, adhere to established protocols, and uphold the values upheld by the OCA. These policies encompass various aspects, including but not limited to administrative procedures, operational protocols, ethical guidelines, and compliance directives.

Designed for all OCA personnel across different departments and functions, these policies and procedures serve as a reference guide to ensure uniformity, compliance, and ethical conduct throughout the organization.

Regular reviews and updates to these policies are scheduled to adapt to evolving needs and to ensure alignment with the OCA's evolving goals. Any proposed changes or updates to these policies will undergo a review process involving relevant departments and administrative bodies within the OCA.

CEO/Director General

Organization Structure

The OCA's organizational structure is meticulously crafted to promote collaboration, transparency, and efficiency in furthering the Olympic Movement's objectives and principles across Asia. This structure comprises four key levels: the Executive Level, the Advisory Level, Core Business Units, and Support Functions.

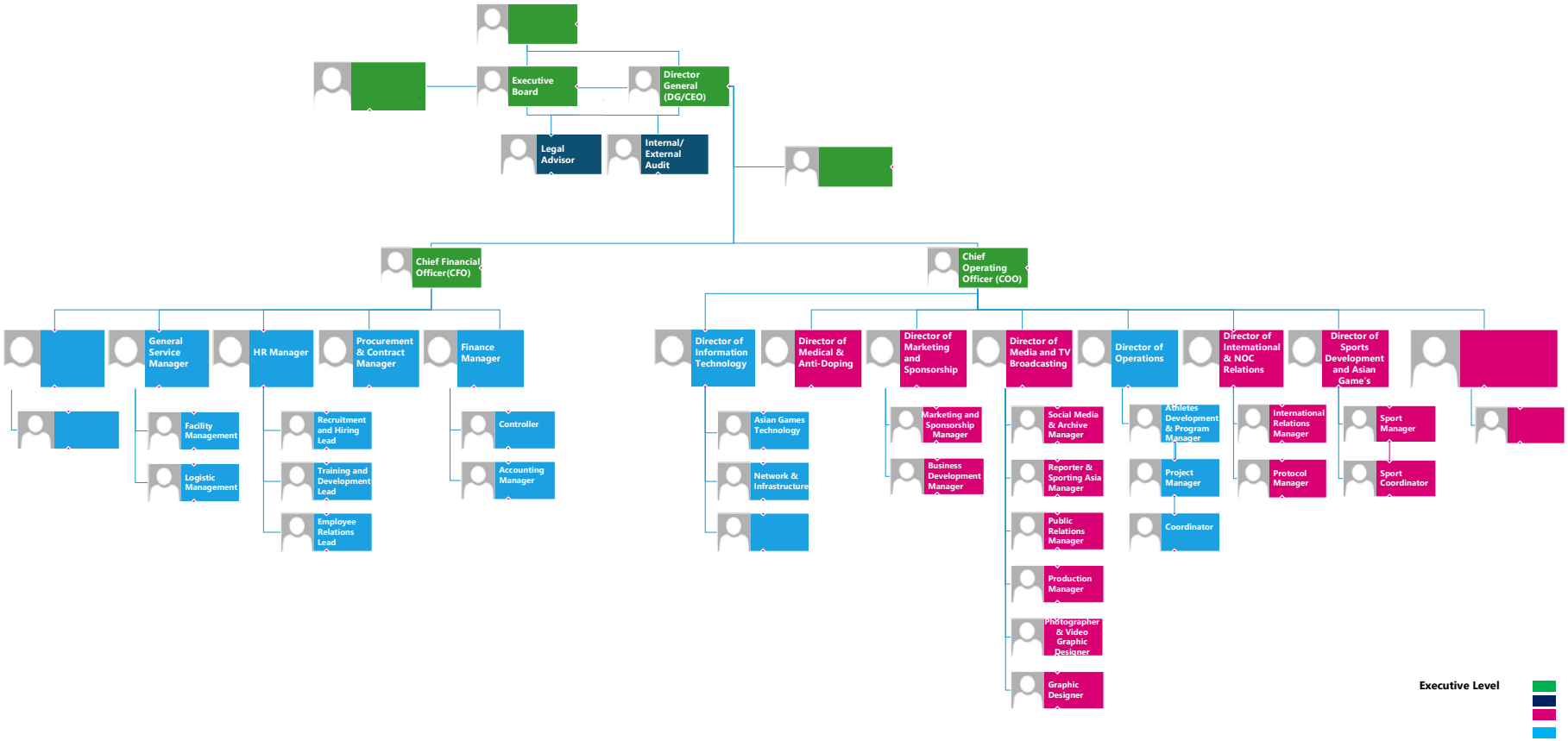
- **Executive Level:** This level is responsible for overall strategic direction, decision-making, and representing the OCA at the highest levels of international sport.

- **Advisory Level:** The Advisory Level includes committees and commissions. These bodies provide expert advice and guidance on specific areas, helping shape policies and programs that align with the OCA's mission.

- **Core Business Units:** Core Business Units are responsible for the day-to-day operations and implementation of the OCA's programs. This includes departments focused on sports development, event management, marketing, and communications, among others.

- **Support Functions:** Support Functions encompass departments such as Finance, Human Resources, Legal Affairs and others. They provide essential services to ensure the smooth functioning of the organization.

Each level of the OCA's organizational structure plays a vital role in advancing the Olympic Movement in Asia. By fostering collaboration and defining clear roles and responsibilities, the structure enables the OCA to effectively fulfill its mission of promoting Olympism and supporting the development of sport in the region.



OCA Organization Structure

Overview and Policy Framework

The Olympic Council of Asia (OCA) operates as a paramount organization dedicated to fostering athletic excellence, promoting cultural exchange, and advancing educational initiatives across the Asian continent. At the core of our operational framework lies a robust set of policies and procedures designed to uphold the highest standards of governance, ethics, security, and operational efficiency.

Mission and Values:

The OCA's mission is to facilitate unity, cooperation, and progress within the Asian sporting community. We are committed to promoting fair play, mutual respect, and the Olympic values of excellence, friendship, and respect. Our policies and procedures are a reflection of these values, emphasizing integrity, inclusivity, and transparency in all our endeavors.

Policy Framework:

The policies and procedures encompassed within this handbook are structured to provide a comprehensive framework that guides the conduct, decision-making, and operations within the OCA. Each policy is meticulously crafted to address specific aspects critical to our organizational success and ethical governance.

Key Policy Domains:

Governance and Ethics: Policies outlining ethical standards, code of conduct for officials, and guidelines for fair and transparent decision-making processes.

Security and Compliance: Measures ensuring the safety of athletes, officials, and stakeholders, alongside compliance with international sports regulations and protocols.

Operational Protocols: Guidelines governing day-to-day operations, event management, resource allocation, and communication standards within the organization.

Financial Governance: Policies pertaining to fiscal responsibility, budgeting, transparency, and risk management to ensure prudent financial practices.

Athlete Welfare and Development: Policies focusing on athlete development, support mechanisms, anti-doping measures, and initiatives promoting fair play and sportsmanship.

Stakeholder Engagement: Guidelines for effective engagement and collaboration with member nations, partners, sponsors, and the wider sporting community.

Importance of Policies:

These policies and procedures serve as the cornerstone of our organizational structure. They provide a common framework to guide decision-making, ensure consistency in operations, mitigate risks, protect the welfare of stakeholders, and uphold the integrity of the OCA and its associated events.

Policies and Procedures

International & NOC Relations Policies and Procedures

OCA is committed to providing the best possible working conditions for its employees.

Purpose

The purpose of the International & NOC Relations policy is to establish a comprehensive framework that governs the relationships between the Olympic Council of Asia (OCA) and international stakeholders, as well as the interactions with its member National Olympic Committees (NOCs). This policy aims to ensure effective collaboration, promote transparency, and foster mutually beneficial partnerships within the global Olympic movement.

Policy

International Relations:

- Collaboration with International Olympic Committee (IOC):
    - The OCA will establish and maintain a positive and productive relationship with the International Olympic Committee (IOC).
    - Clear procedures will be defined for regular communication, coordination, and collaboration with the IOC on matters related to sports development, Olympic Games participation, and policy implementation.
    - The OCA will adhere to the IOC's principles, guidelines, and regulations to ensure alignment and compliance with the global Olympic movement.

- Engagement with International Sports Federations (IFs):
    - The OCA will actively engage with International Sports Federations (IFs) to promote and develop Olympic sports within the region.
    - Procedures will be established for effective communication, exchange of information, and collaboration with IFs on matters related to sports development, competitions, and technical regulations.

- The OCA will support and encourage the participation of member NOCs in IF activities, including conferences, workshops, and training programs.

- International Sports Event Hosting:
  - The OCA will establish procedures and criteria for the bidding and hosting of international sports events within the region.
  - Transparent and fair selection processes will be implemented to ensure equal opportunities for member NOCs to host major international events.
  - The OCA will provide support and guidance to member NOCs in the preparation, organization, and execution of international sports events, ensuring compliance with international standards and regulations.

- National Olympic Committee (NOC) Relations:
  - Membership and Governance:
    - The OCA will establish procedures and criteria for the recognition and membership of National Olympic Committees (NOCs) within the region.
    - Clear guidelines will be provided for the establishment and governance of NOCs, ensuring compliance with the Olympic Charter and OCA regulations.
    - The OCA will support NOCs in enhancing their governance structures, operational capacities, and financial sustainability.

  - NOC Collaboration and Exchange:
    - The OCA will facilitate collaboration and exchange programs among member NOCs, encouraging the sharing of best practices, knowledge, and experiences.
    - Procedures will be established for the organization of NOC conferences, workshops, and seminars to foster networking, learning, and collaboration among NOCs.
    - The OCA will provide support and resources to NOCs for athlete and coach development, sports infrastructure improvement, and capacity-building initiatives.

- Support and Assistance to NOCs:
  - The OCA will establish procedures for providing support and assistance to member NOCs in their Olympic activities and programs.
  - Clear guidelines will be provided for NOC funding, scholarships, and grants, aiming to strengthen the operational capabilities and performance of NOCs.
  - The OCA will offer technical expertise, resources, and guidance to NOCs in the areas of sports administration, marketing and sponsorship, sports science, and sports medicine.

- Policy Compliance and Monitoring:
  - The OCA will establish procedures and mechanisms for monitoring the compliance of member NOCs with OCA regulations and policies.
  - Regular assessments and audits will be conducted to ensure that NOCs adhere to ethical standards, good governance practices, and anti-doping regulations.
  - The OCA will provide support and resources to NOCs to enhance their capacity for policy implementation and compliance.

- Information Sharing and Communication:
  - The OCA will establish procedures for effective communication and information sharing with member NOCs, ensuring timely dissemination of relevant updates, policies, and guidelines.
  - Clear channels of communication, such as official websites, newsletters, and online platforms, will be established to facilitate efficient and transparent communication between the OCA and NOCs.
  - The OCA will encourage NOCs to provide feedback, suggestions, and reports on their activities, challenges, and achievements to foster a collaborative and constructive relationship.

Procedures

- International Relations:
    - Collaboration with International Olympic Committee (IOC):
        - The OCA will establish a dedicated point of contact and communication channels with the IOC.
        - Regular meetings, both in-person and virtual, will be scheduled to discuss and align on strategic matters.
        - The OCA will actively participate in IOC conferences, workshops, and forums to stay updated on global Olympic movement initiatives.
        - The OCA will promptly respond to IOC inquiries and requests for information or assistance.

    - Engagement with International Sports Federations (IFs):
        - The OCA will maintain a database of contact information for all relevant International Sports Federations (IFs).
        - Regular communication will be established with IFs to exchange information, seek guidance, and share updates on regional sports development.
        - The OCA will encourage member NOCs to establish direct communication channels with respective IFs for effective collaboration.
        - The OCA will coordinate with IFs to facilitate technical support visits, training programs, and educational workshops within the region.

    - International Sports Event Hosting:
        - The OCA will establish a transparent and standardized bidding process for hosting international sports events.
        - The OCA will issue clear guidelines and criteria for evaluating bids, including infrastructure requirements, financial capabilities, and hosting experience.

- A designated evaluation committee will review and assess the bids based on predetermined criteria and visit proposed venues for inspection.
- The OCA will provide support and guidance to the selected host NOC in event planning, organization, and delivery, including logistical arrangements, protocol, and promotion.

- National Olympic Committee (NOC) Relations:
  - Membership and Governance:
    - The OCA will establish an application process for NOC membership, including submission of required documentation and compliance with eligibility criteria.
    - An evaluation committee will review membership applications and make recommendations to the OCA Executive Board for final approval.
    - The OCA will provide guidance and support to newly established NOCs for the development of their governance structures, constitutions, and election processes.
    - Regular audits and compliance checks will be conducted to ensure that member NOCs adhere to the Olympic Charter and OCA regulations.

  - NOC Collaboration and Exchange:
    - The OCA will organize regular NOC conferences, seminars, and workshops to facilitate collaboration and exchange of best practices among member NOCs.
    - Member NOCs will be encouraged to share success stories, challenges, and lessons learned through presentations and panel discussions.
    - The OCA will establish a platform for NOCs to connect and engage in online discussions, share resources, and seek advice from their counterparts.

        - The OCA will allocate funding and resources to support joint projects, talent development initiatives, and regional sports programs involving multiple NOCs.

    - Support and Assistance to NOCs:
        - The OCA will establish a support desk to address inquiries and requests for assistance from member NOCs.
        - Member NOCs will be provided with guidelines and application procedures for accessing available funding, scholarships, and grants.
        - The OCA will conduct capacity-building workshops and training programs for NOC administrators, focusing on areas such as sports administration, marketing, and event management.
        - The OCA will establish a system for monitoring the utilization of allocated funds and evaluating the impact of support programs.

- Policy Compliance and Monitoring:
    - The OCA will establish a dedicated compliance department responsible for monitoring NOCs' compliance with OCA regulations and policies.
    - The compliance department will conduct regular assessments and audits of member NOCs, including financial audits, governance reviews, and adherence to anti-doping regulations.
    - Non-compliance issues will be addressed through a structured process, including warning letters, corrective action plans, and, if necessary, sanctions or suspensions.
    - The compliance department will provide support and guidance to NOCs to rectify compliance issues and improve their governance practices.

- Information Sharing and Communication:
    - The OCA will establish a dedicated information management system to facilitate efficient communication with member NOCs.
    - A central repository will be maintained for storing and disseminating relevant policies, guidelines, and updates to member NOCs.

- Regular newsletters, bulletins, or email updates will be sent to NOCs to provide timely information on upcoming events, policy changes, and other relevant news.
- The OCA will organize annual or biennial meetings with NOC representatives to discuss important matters, share updates, and gather feedback.

- International Relations:
  - Collaboration with International Olympic Committee (IOC):
    - Establish a dedicated International Relations Department within the OCA responsible for managing the collaboration with the IOC.
    - Designate a liaison officer as the main point of contact between the OCA and the IOC.
    - Develop a communication plan outlining regular meeting, conferences, and reporting mechanisms to ensure effective coordination.
    - Maintain a comprehensive record of all communications and agreements with the IOC.

  - Engagement with International Sports Federations (IFs):
    - Establish a database of International Sports Federations (IFs) and their respective contact information.
    - Develop a proactive engagement plan to establish strong working relationships with IFs.
    - Arrange regular meetings, both in-person and virtual, with IF representatives to discuss matters of mutual interest.
    - Collaborate with IFs to organize joint initiatives, such as training programs, seminars, and workshops.

  - International Sports Event Hosting:
    - Develop clear guidelines and criteria for hosting international sports events within the region.
    - Promote the bidding process and provide detailed bid documentation to interested member NOCs.

- Establish an evaluation committee to review bids based on predetermined criteria and visit proposed venues for assessment.
- Provide support and guidance to the selected host NOC in event planning, logistics, marketing, and coordination with relevant stakeholders.

- National Olympic Committee (NOC) Relations:
  - Membership and Governance:
    - Establish a membership application process outlining the required documentation and eligibility criteria for NOCs.
    - Form a Membership Committee responsible for reviewing and evaluating membership applications.
    - Conduct due diligence on prospective NOCs, including their governance structures and compliance with the Olympic Charter.
    - Present the findings and recommendations to the OCA Executive Board for final approval of NOC membership.

  - NOC Collaboration and Exchange:
    - Organize regular NOC conferences, seminars, and workshops to foster collaboration and knowledge-sharing among member NOCs.
    - Encourage member NOCs to share best practices, success stories, and challenges through presentations and interactive sessions.
    - Establish a platform for NOCs to connect and communicate online, facilitating ongoing collaboration and information exchange.
    - Allocate funds for joint projects and initiatives involving multiple NOCs to promote cooperation and regional sports development.

  - Support and Assistance to NOCs:
    - Develop clear guidelines and application procedures for NOCs to access support and assistance programs.
    - Establish a dedicated Support and Assistance Department within the OCA responsible for managing these programs.
    - Provide financial resources, scholarships, and grants to NOCs based on predetermined criteria and priorities.

        - Conduct capacity-building workshops, training programs, and mentorship initiatives to enhance NOC capabilities in various areas, including sports administration, governance, and marketing.

- Policy Compliance and Monitoring:
    - Establish a Compliance Department within the OCA responsible for monitoring NOCs' compliance with OCA regulations and policies.
    - Develop a compliance framework outlining the processes, tools, and criteria for assessing NOCs' compliance.
    - Conduct regular audits and assessments of NOCs' activities, governance practices, and financial management to ensure compliance.
    - Implement a system of reporting and documentation to track compliance status, identified issues, and corrective actions taken.
    - Enforce a progressive disciplinary system for non-compliant NOCs, including warning letters, suspension, or revocation of membership.

- Information Sharing and Communication:
    - Establish an Information Management System to centralize communication and information sharing with member NOCs.
    - Develop a communication plan that includes regular newsletters, bulletins, and official communications to member NOCs.
    - Maintain an up-to-date website and online platform to provide NOCs with access to relevant policies, guidelines, and updates.
    - Organize periodic meetings and conferences with NOC representatives to discuss important matters, share updates, and gather feedback.
    - Foster a culture of open communication and responsiveness, ensuring timely responses to inquiries and requests from member NOCs.

Medical & Anti-Doping Policies and Procedures

Purpose

The purpose of this policy is to establish clear guidelines, procedures, and regulations regarding medical and anti-doping practices within the Olympic Council of Asia (OCA). This policy aims to promote the health, well-being, and fair competition of athletes participating in OCA events, while upholding the highest standards of integrity and sportsmanship. By implementing comprehensive medical and anti-doping policies, the OCA seeks to ensure a level playing field, protect athletes' rights, and maintain the credibility of sports competitions under its jurisdiction. This policy serves as a framework to guide athletes, coaches, medical personnel, and other stakeholders in adhering to the principles of ethical and clean sport, emphasizing the importance of athlete welfare, anti-doping education, pre-participation medical assessments, anti-doping testing procedures, and appropriate medical support during OCA events. The OCA is committed to continually reviewing and enhancing these policies to align with international standards and best practices in sports medicine and anti-doping, fostering a culture of integrity, fairness, and excellence in Asian sports.

Policy

- Pre-Participation Medical Assessment:
    - All athletes participating in OCA events must undergo a comprehensive pre-participation medical assessment conducted by qualified medical professionals.
    - The assessment should include a thorough medical history review, physical examination, and any necessary diagnostic tests to determine the athlete's fitness to compete.

- Medical Support during OCA Events:
    - The OCA shall ensure the availability of appropriate medical support, including qualified medical personnel, first aid services, and necessary medical facilities at all OCA-sanctioned events.
    - Adequate emergency response protocols and equipment must be in place to address any medical emergencies that may arise during competitions.

- Prohibited Substances and Methods:
    - The use of substances and methods prohibited by the World Anti-Doping Agency (WADA) is strictly prohibited within the OCA's jurisdiction.
    - A comprehensive list of prohibited substances and methods, as outlined by the WADA Code, should be provided to all athletes, coaches, and support staff.
    - Athletes are responsible for ensuring they do not use any banned substances or methods and should seek appropriate medical advice to avoid unintentional violations.

- Doping Control and Testing:
    - The OCA shall implement robust doping control and testing procedures to detect and deter the use of prohibited substances or methods.
    - Random and targeted testing programs should be conducted, covering both in-competition and out-of-competition periods.
    - The testing process should adhere to the guidelines and protocols established by WADA, including sample collection, storage, transportation, and analysis.

- Therapeutic Use Exemptions (TUEs):
    - Athletes requiring the legitimate use of medications or treatments that contain prohibited substances must obtain a Therapeutic Use Exemption (TUE) from the appropriate authorities.
    - The process for applying for TUEs should be clearly outlined, including the required documentation and review procedures.

- Education and Awareness:
    - The OCA shall develop and implement educational programs on anti-doping, providing athletes, coaches, and support staff with information about the risks and consequences of doping.
    - Regular anti-doping workshops, seminars, and awareness campaigns should be organized to ensure ongoing education and compliance.

- Results Management:
    - Adverse analytical findings and anti-doping rule violations should be handled in accordance with established disciplinary procedures and WADA guidelines.
    - Sanctions, including disqualification, suspension, or other appropriate penalties, should be implemented consistently and fairly.

- Confidentiality and Data Protection:
    - The OCA must ensure the strict confidentiality of medical and anti-doping information, adhering to applicable privacy and data protection laws.
    - Access to athlete medical records and anti-doping test results should be limited to authorized individuals or entities involved in the management and enforcement of the policy.

- Compliance and Reporting:
    - The OCA shall monitor and enforce compliance with the medical and anti-doping policies, conducting regular audits and assessments.
    - Any suspected or actual violations of the policy should be reported to the appropriate authorities and handled in accordance with established procedures.

- Policy Review and Updates:
    - The medical and anti-doping policies should be periodically reviewed to ensure their alignment with the latest WADA Code and international standards.
    - Feedback from athletes, coaches, medical professionals, and other stakeholders should be considered when making updates or amendments to the policy.

Procedures

- Pre-Participation Medical Assessment:
    - Athletes must complete a detailed medical history form, providing accurate and comprehensive information about their medical conditions, previous injuries, and any ongoing treatments.
    - Qualified medical professionals will conduct a thorough physical examination, including measurements of vital signs, musculoskeletal assessments, and cardiovascular screenings.
    - Diagnostic tests, such as blood tests, imaging studies, or specialized evaluations, may be requested based on individual athlete needs or specific sport requirements.
    - The medical assessment findings and recommendations should be documented in the athlete's medical records, including any identified medical concerns or recommendations for further evaluation or treatment.

- Medical Support during OCA Events:
    - The OCA will appoint a medical coordinator or team responsible for coordinating medical services at OCA-sanctioned events.
    - Adequate medical personnel, including physicians, nurses, physiotherapists, and athletic trainers, should be available during events.
    - Medical personnel should be properly trained in sports medicine, emergency response, and injury management.
    - Medical facilities, first aid stations, and necessary medical equipment must be provided at event venues.
    - An emergency action plan (EAP) should be developed and communicated to all relevant stakeholders, outlining procedures for handling medical emergencies, including immediate care, emergency medical transportation, and communication with medical facilities.

- Prohibited Substances and Methods:
    - The OCA will maintain an up-to-date list of prohibited substances and methods, consistent with the WADA Code.
    - Athletes, coaches, and support staff should receive regular education and training on the list of banned substances and methods.
    - The OCA should establish clear guidelines on the proper use of medications and supplements, emphasizing the importance of obtaining necessary approvals and avoiding prohibited substances.
    - Athletes should consult with qualified healthcare professionals and adhere to the principles of clean sport, taking responsibility for their own compliance with anti-doping regulations.

- Doping Control and Testing:
    - The OCA will collaborate with national anti-doping agencies and accredited laboratories to conduct doping control testing.
    - Random and targeted testing plans should be developed, covering both in-competition and out-of-competition periods.
    - Athletes will be notified of their selection for testing and provided with information on the testing process and their rights and responsibilities.
    - Doping control officers will collect samples from athletes in accordance with WADA guidelines, ensuring proper chain of custody and maintaining sample integrity during transportation to accredited laboratories.
    - Sample analysis will be conducted by certified laboratories, following established protocols and procedures.
    - Athletes will have the right to request the presence of a representative during sample collection and can provide additional information or request B-sample analysis if necessary.

- Therapeutic Use Exemptions (TUEs):
    - The OCA will establish a TUE Committee responsible for reviewing and approving TUE applications.
    - Athletes requiring the legitimate use of medications or treatments containing prohibited substances must submit a TUE application along with supporting medical documentation.

- The TUE Committee will review applications based on the WADA TUE criteria and provide a timely decision.
- Approved TUEs will be granted for a specified duration, and athletes will be responsible for renewing their TUEs when necessary.

- Education and Awareness:
  - The OCA will develop and implement educational programs and workshops on anti-doping and sports medicine for athletes, coaches, and support staff.
  - Educational materials, including brochures, handbooks, and online resources, will be provided to enhance awareness and understanding of anti-doping regulations and medical best practices.
  - Collaboration with national anti-doping agencies and international organizations will be sought to ensure access to comprehensive and up-to-date educational materials.
  - Athletes and support personnel will be required to complete anti-doping education modules and demonstrate their knowledge and understanding of anti-doping regulations.

- Results Management:
  - The OCA will establish a Results Management Committee responsible for handling adverse analytical findings and anti-doping rule violations.
  - Adverse findings will be communicated to the athlete and their national anti-doping agency, initiating the results management process.
  - Athletes will have the opportunity to provide explanations or request analysis of the B-sample.
  - Disciplinary hearings will be conducted, affording athletes the opportunity to present their case and provide evidence.
  - Sanctions, including disqualification, suspension, or other appropriate penalties, will be imposed in accordance with WADA guidelines and the severity of the violation.
  - Appeals processes will be provided for athletes who wish to challenge the decisions through established channels.

- Confidentiality and Data Protection:
    - The OCA will implement strict protocols to ensure the confidentiality and protection of athlete medical records and anti-doping information.
    - Access to medical records and anti-doping test results will be limited to authorized personnel involved in the management, testing, or enforcement of the policy.
    - Appropriate data protection measures, including secure storage, access controls, and encryption, will be implemented to safeguard athlete information.
    - Athletes will be informed of their rights regarding data privacy and given the opportunity to review and update their personal information.

- Compliance and Reporting:
    - The OCA will establish a compliance monitoring program to ensure adherence to the medical and anti-doping policies.
    - Regular audits and assessments will be conducted to identify any non-compliance and take corrective actions as necessary.
    - Suspected or actual violations of the policy will be reported to the appropriate national or international anti-doping agencies, as required.
    - Whistleblower provisions and reporting mechanisms should be in place to encourage the reporting of any potential violations.

- Policy Review and Updates:
    - The OCA will conduct periodic reviews of the medical and anti-doping policies to ensure alignment with the latest WADA Code and international standards.
    - Stakeholder feedback, including athletes, coaches, medical professionals, and anti-doping experts, will be solicited to inform updates and amendments.
    - The policy review process will involve consultation with legal experts and international sports governing bodies to ensure compliance with regulations and best practices.

Development And Athlete Performance Policies and Procedures

Purpose

The purpose of this Development and Athlete Performance policy is to provide a comprehensive framework for the identification, development, and support of talented athletes within the Olympic Council of Asia (OCA) member countries. This policy aims to foster the growth and excellence of athletes by establishing clear guidelines and procedures for talent identification, long-term athlete development, coaching standards, and athlete support services. By implementing this policy, the OCA seeks to promote a systematic and progressive approach to athlete development, ensuring that talented individuals are given the necessary resources, training, and support to reach their full potential. The policy also emphasizes the importance of collaboration with national sports federations, coaches, and relevant stakeholders to create a unified and effective approach to athlete development across the region. The OCA is committed to monitoring and evaluating the implementation of this policy to ensure its effectiveness and continuous improvement. Ultimately, the purpose of this policy is to contribute to the development of a strong and competitive athlete base within the OCA, fostering a culture of excellence and promoting the values of sport throughout the region.

Policy

- Talent Identification and Development:
  - Talent Identification Programs:
    - The OCA will establish talent identification programs aimed at identifying and nurturing young athletes with potential for excellence in sports.
    - Clear criteria and processes will be defined for talent identification, including talent camps, trials, performance assessments, and consultation with coaches and experts.
    - Collaboration with national sports federations and regional bodies will be encouraged to ensure comprehensive talent identification across member countries.

- Development Pathway:
  - The OCA will provide a development pathway for identified talents, focusing on their long-term athletic development and progression.
  - Specialized training programs, coaching support, and access to appropriate facilities and resources will be provided to support the development of identified talents.
  - Regular monitoring and evaluation will be conducted to track the progress and performance of identified talents, and necessary adjustments to their development plans will be made accordingly.

- Long-Term Athlete Development (LTAD):
  - LTAD Framework:
    - The OCA will establish a comprehensive Long-Term Athlete Development (LTAD) framework that outlines the stages and components of athlete development.
    - The LTAD framework will consider the age, physical and mental development, and competition readiness of athletes, providing guidelines for their systematic and progressive development.
    - The framework will include key aspects such as training and competition loads, rest and recovery periods, skill acquisition, and performance enhancement strategies at each stage of the athlete's development.

  - Integration with National Federations:
    - The OCA will collaborate with national sports federations to ensure the implementation of LTAD principles at the national level.
    - National federations will be encouraged to align their athlete development programs with the OCA's LTAD framework, fostering a coordinated and consistent approach to athlete development across member countries.
    - Support and resources will be provided to national federations to facilitate the implementation of LTAD programs and ensure their effectiveness.

- Coaching and Athlete Support:
    - Coaching Standards:
        - The OCA will establish coaching standards and guidelines to ensure the provision of qualified and competent coaches for athlete development programs.
        - Criteria and processes for coach selection, certification, and ongoing professional development will be defined, emphasizing the importance of continuous learning and adherence to ethical coaching practices.
        - Collaboration with national coaching bodies and international coaching organizations will be encouraged to promote the sharing of best practices and the professional growth of coaches.

    - Athlete Support Services:
        - The OCA will strive to provide comprehensive athlete support services, including sports science, sports medicine, and mental health support, to enhance athlete performance and well-being.
        - Collaboration with relevant stakeholders, such as sports institutes, medical professionals, and sports psychologists, will be sought to ensure the availability of high-quality support services for athletes.
        - Athletes will have access to resources and programs aimed at optimizing their physical, technical, tactical, and psychological development.

- Monitoring and Evaluation:
    - The OCA will implement a robust monitoring and evaluation system to assess the effectiveness and impact of development and athlete performance programs.
    - Regular data collection, analysis, and reporting will be conducted to track the progress, achievements, and challenges of athletes and the effectiveness of the implemented policies.
    - Feedback mechanisms from athletes, coaches, and other stakeholders will be established to gather insights and suggestions for program improvement.

Procedures

- Talent Identification and Development:
    - Talent Identification Programs:
        - The OCA will establish clear procedures for the implementation of talent identification programs.
        - Detailed guidelines and criteria for talent identification, including age ranges, performance benchmarks, and evaluation methods, will be established.
        - The OCA will collaborate with national sports federations and regional bodies to organize talent camps, trials, and assessments.
        - Regular reviews and updates of the talent identification procedures will be conducted to ensure their effectiveness.

    - Development Pathway:
        - Once talents are identified, a well-defined development pathway will be established.
        - Procedures for assigning identified talents to specialized training programs, including coaching and support services, will be put in place.
        - Individualized development plans will be created for each talent, outlining their short-term and long-term goals, training schedules, and performance evaluation methods.
        - Regular monitoring and evaluation will be conducted to track the progress and performance of identified talents, with adjustments made to their development plans as needed.
- Long-Term Athlete Development (LTAD):
    - LTAD Framework Implementation:
        - The OCA will establish clear procedures for the implementation of the LTAD framework.
        - Detailed guidelines and recommendations for each stage of athlete development, including training volume, intensity, and progression, will be provided.

        - National sports federations will be responsible for implementing the LTAD framework within their respective countries, following the guidelines set by the OCA.
        - Regular communication and collaboration between the OCA and national federations will be encouraged to ensure the effective implementation of the LTAD framework.

    - Integration with National Federations:
        - Procedures for collaboration between the OCA and national federations will be established to align athlete development programs with the LTAD framework.
        - Guidelines for sharing resources, expertise, and best practices between the OCA and national federations will be developed.
        - National federations will be required to submit progress reports on their implementation of LTAD programs, including athlete monitoring data and program evaluation results.

- Coaching and Athlete Support:
    - Coaching Standards:
        - The OCA will establish clear procedures for coach selection, certification, and ongoing professional development.
        - Detailed guidelines for coach qualification criteria, application processes, and required certifications will be provided.
        - The OCA will establish partnerships with relevant coaching bodies to ensure that coaches receive appropriate training and support.
        - Regular audits and assessments of coaching standards will be conducted to maintain the quality and professionalism of coaches.
    - Athlete Support Services:
        - The OCA will establish procedures for the provision of comprehensive athlete support services.
        - Detailed guidelines for the availability of sports science, sports medicine, and mental health support services will be developed.

- Collaboration with relevant stakeholders, such as sports institutes and medical professionals, will be established to ensure the provision of high-quality support services.
- Athletes will be provided with clear procedures to access support services, including assessment procedures, referral mechanisms, and follow-up protocols.

- Monitoring and Evaluation:
  - The OCA will establish procedures for monitoring and evaluating the effectiveness of development and athlete performance programs.
  - Data collection protocols, including performance metrics, athlete evaluations, and program feedback, will be established.
  - Regular analysis and reporting of the collected data will be conducted to assess the progress, achievements, and challenges of athletes and the effectiveness of the implemented policies.
  - Procedures for gathering feedback from athletes, coaches, and other stakeholders through surveys, interviews, or focus groups will be established.

Media And TV Broadcasting Policies and Procedures

Purpose

The purpose of this Media and TV Broadcasting policy is to establish guidelines and procedures that ensure professional and responsible media coverage of OCA events. This policy aims to promote transparency, fairness, and accuracy in media reporting, while safeguarding the intellectual property rights and privacy of athletes and officials. By setting clear standards for media accreditation, operations, broadcasting, and ethical conduct, this policy seeks to maintain the integrity and positive image of OCA events, while providing accredited media organizations with the necessary access and opportunities to cover and promote these events. The policy also emphasizes compliance with international broadcasting regulations and intellectual property rights, fostering a collaborative and respectful relationship between the OCA, media organizations, and other stakeholders. This policy will be regularly reviewed and updated to reflect the evolving media landscape, industry best practices, and the OCA's commitment to excellence in media and TV broadcasting.

Policy

- Media Accreditation:
    - Accreditation Process:
        - The policy should outline the criteria and procedures for media organizations to apply for accreditation to cover OCA events.
        - Media organizations will be required to submit an application form along with relevant documentation, such as proof of affiliation, professional credentials, and a code of conduct agreement.
        - The OCA will review and evaluate applications based on established criteria, including the organization's track record, journalistic ethics, and commitment to fair and accurate reporting.
        - Approved media organizations will receive accreditation badges or credentials, granting them access to designated media areas, press conferences, and interview opportunities.

- Rights and Responsibilities:
  - The policy should clearly outline the rights and responsibilities of accredited media personnel.
  - Rights may include access to event venues, press facilities, mixed zones, and designated interview areas.
  - Responsibilities may include adhering to ethical standards, respecting athlete privacy, following venue regulations, and complying with OCA media guidelines.
  - Media personnel should be responsible for ensuring accurate and fair reporting, respecting intellectual property rights, and complying with relevant laws and regulations.

- Media Operations:
  - Venue Access and Facilities:
    - The policy should define the areas and facilities available to accredited media personnel within event venues, including media centers, press rooms, and designated workspaces.
    - Guidelines should be provided for access control, security procedures, and allocation of workspace or broadcasting positions.
  - Adequate infrastructure, such as internet connectivity, power supply, and media services, should be provided to support media operations.

  - Press Conferences and Interviews:
    - Procedures for organizing press conferences, media briefings, and interview sessions should be outlined in the policy.
    - The policy should define the process for requesting and conducting interviews with athletes, coaches, and officials.
    - Guidelines should be provided regarding the use of recording devices, photography, and video broadcasting during press conferences and interviews.
  - Broadcasting and Reporting Guidelines:
    - The policy should establish guidelines for media organizations regarding broadcasting rights, restrictions, and usage of OCA event footage, images, and content.

- Media organizations should be required to obtain appropriate broadcasting licenses and permissions before transmitting live coverage or recorded content of OCA events.
- Guidelines should be provided for accurate and responsible reporting, including fact-checking, attribution of sources, and respect for cultural sensitivities.
- Guidelines on the use of social media, including the proper attribution of content and engagement with followers, should be included.

- Intellectual Property Rights:
  - The policy should emphasize the importance of respecting intellectual property rights associated with OCA events.
  - Media organizations should be prohibited from using OCA logos, trademarks, or event-related content without prior authorization.
  - Clear guidelines should be provided regarding the use of OCA event footage, images, and branding, including proper attribution and compliance with licensing agreements.

- Ethics and Professionalism:
  - The policy should emphasize adherence to professional ethics, including accuracy, fairness, and impartiality in reporting.
  - Media organizations should be required to abide by relevant journalism ethics codes and industry best practices.
  - Guidelines should be provided regarding privacy protection, especially when it comes to personal information and interviews with athletes and officials.
  - Media personnel should conduct themselves in a professional and respectful manner, maintaining decorum during interviews, press conferences, and other media interactions.
- Compliance and Enforcement:
  - The policy should outline the consequences for violations of the media and TV broadcasting policy, including potential revocation of accreditation and legal actions.

- A reporting mechanism should be established for stakeholders to submit complaints or concerns regarding media coverage and conduct.
- The OCA should have a designated committee or authority responsible for monitoring and enforcing compliance with the policy.

- Policy Review and Updates:
  - The policy should state that it will be periodically reviewed and updated to reflect changes in media technology, industry standards, and regulatory requirements.
  - Feedback and suggestions from media organizations, athletes, officials, and other stakeholders should be considered during the policy review process.

Procedures

- Media Accreditation:
  - Accreditation Process:
    - The OCA will establish a dedicated accreditation portal or system for media organizations to apply for accreditation to cover OCA events.
    - Media organizations will be required to complete an online application form, providing detailed information about their organization, including their media credentials, affiliation, and contact details.
    - The OCA's accreditation committee will review the applications and verify the provided information.
    - Once approved, media organizations will receive confirmation of their accreditation along with instructions for badge collection or digital credentials.

  - Accreditation Badges/Credentials:
    - Accredited media personnel will be required to collect their accreditation badges or credentials from a designated accreditation center or location.

- Media personnel must present a valid identification document and a confirmation email or reference number during the badge collection process.
- Badges should clearly display the media organization's name, the individual's name, photograph, and the validity period of the accreditation.
- Accreditation badges should be worn visibly at all times when accessing event venues and media areas.

  - Media Accreditation Rights and Responsibilities:
    - The policy should clearly outline the rights and responsibilities of accredited media personnel.
    - Rights may include access to designated media areas, press conferences, mixed zones, interview opportunities, and official events.
    - Responsibilities may include adhering to ethical standards, respecting athlete privacy, following venue regulations, and complying with OCA media guidelines.
    - Media personnel should be responsible for ensuring accurate and fair reporting, respecting intellectual property rights, and complying with relevant laws and regulations.

- Media Operations:
  - Venue Access and Facilities:
    - The OCA will designate specific media areas within event venues, such as media centers, press rooms, and designated workspaces.
    - Accredited media personnel will be granted access to these designated areas upon presentation of their valid accreditation badges or credentials.
    - Access control measures, including security checks, may be implemented to ensure the safety and integrity of the event.
    - Adequate infrastructure, such as internet connectivity, power supply, and media services, will be provided to support media operations in designated areas.

- Press Conferences and Interviews:
  - The OCA will schedule and organize press conferences and media briefings with key stakeholders, including athletes, coaches, and officials.
  - Media organizations will be notified of the press conference schedule and given the opportunity to request specific interviews.
  - During press conferences and interviews, media personnel must follow any guidelines provided by the OCA, such as designated seating arrangements, time limits for questions, and restrictions on photography or recording.
  - Respectful and professional conduct should be maintained during press conferences and interviews, including adherence to any cultural sensitivities.

- Broadcasting and Reporting Guidelines:
  - Media organizations intending to broadcast OCA events live or record footage for later use must obtain appropriate broadcasting licenses and permissions.
  - Guidelines on the use of OCA event footage, images, and branding should be provided to ensure compliance with intellectual property rights.
  - Media organizations should follow accurate and responsible reporting practices, including fact-checking, proper attribution of sources, and verification of information.
  - Guidelines on the use of social media platforms, including the proper attribution of content, engagement with followers, and compliance with platform policies, should be provided.

- Intellectual Property Rights:
  - Media organizations should respect intellectual property rights associated with OCA events.
  - The policy should clearly state that the use of OCA logos, trademarks, or event-related content without prior authorization is strictly prohibited.

- Guidelines on the use of OCA event footage, images, and branding should be provided, emphasizing proper attribution, compliance with licensing agreements, and respect for intellectual property rights.

- Ethics and Professionalism:
  - Media organizations should adhere to professional ethics, including accuracy, fairness, and impartiality in reporting.
  - Compliance with relevant journalism ethics codes and industry best practices should be emphasized.
  - Guidelines should be provided to media personnel regarding privacy protection, especially when it comes to personal information and interviews with athletes and officials.
  - Media personnel should conduct themselves in a professional and respectful manner, maintaining decorum during interviews, press conferences, and other media interactions.

- Compliance and Enforcement:
  - The OCA will establish a designated committee or authority responsible for monitoring and enforcing compliance with the media and TV broadcasting policy.
  - The committee or authority will conduct regular monitoring and audits to ensure media organizations adhere to the policy guidelines.
  - Any reported violations or non-compliance with the policy will be investigated by the committee or authority, and appropriate actions will be taken, including warning, suspension, or revocation of accreditation.
  - A reporting mechanism should be established for stakeholders to submit complaints or concerns regarding media coverage and conduct.

- Policy Review and Updates:
  - The policy should state that it will be periodically reviewed and updated to reflect changes in media technology, industry standards, and regulatory requirements.

- Feedback and suggestions from media organizations, athletes, officials, and other stakeholders should be considered during the policy review process.

The policy review process may involve consultation with legal experts, media professionals, and relevant authorities to ensure compliance with regulations and best practices.

Marketing & Sponsorship Policies and Procedures

Purpose

The OCA is responsible for organizing the Asian Games, the Asian Winter Games, and other regional sporting events. The Marketing and Sponsorship Department of the OCA is responsible for generating revenue for the OCA through the sale of marketing and sponsorship rights.

The Marketing and Sponsorship Department is responsible for developing and implementing a marketing and sponsorship strategy that aligns with the OCA's overall goals and objectives. The department is also responsible for negotiating and executing marketing and sponsorship agreements, and for managing the relationships with the OCA's marketing and sponsorship partners.

Policy

Marketing and Sponsorship Strategy

The OCA's marketing and sponsorship strategy should be aligned with the OCA's overall goals and objectives. The strategy should be developed in consultation with the OCA's Executive Board and should be reviewed on a regular basis to ensure that it is still relevant and appropriate.

The OCA's marketing and sponsorship strategy should include the following elements:

- A target audience: The OCA should identify its target audience for marketing and sponsorship. This audience could include fans of the Olympic Movement, athletes, sponsors, broadcasters, and other stakeholders.
- Marketing messages: The OCA should develop marketing messages that are relevant to its target audience. These messages should communicate the OCA's brand, values, and mission.
- Marketing channels: The OCA should select marketing channels that will reach its target audience. These channels could include print, television, digital, and social media.
- Marketing budget: The OCA should allocate a budget for marketing and sponsorship. This budget should be based on the OCA's goals and objectives, as well as the cost of marketing and sponsorship activities.
- Sponsorship opportunities: The OCA should identify sponsorship opportunities that are aligned with its marketing and sponsorship strategy. These opportunities could include naming rights, sponsorship of events, and product placement.
- Sponsorship criteria: The OCA should establish criteria for evaluating potential sponsorship partners. These criteria could include the partner's financial resources, brand alignment, and commitment to the Olympic Movement.
- Sponsorship terms and conditions: The OCA should develop terms and conditions for sponsorship agreements. These terms and conditions should protect the OCA's interests and ensure that the partnership is mutually beneficial.

Marketing and Sponsorship Agreements

The OCA's marketing and sponsorship agreements should be negotiated and executed in accordance with the OCA's policies and procedures. The agreements should be in writing and should be signed by authorized representatives of the OCA and the OCA's marketing and sponsorship partners.

The OCA's marketing and sponsorship agreements should include the following elements:

- The parties to the agreement: The agreement should identify the OCA and the marketing and sponsorship partner.
- The term of the agreement: The agreement should specify the term of the partnership.
- The scope of the agreement: The agreement should specify the scope of the partnership, including the rights and obligations of the parties.
- The rights and obligations of the parties: The agreement should specify the rights and obligations of the OCA and the marketing and sponsorship partner.
- The payment terms: The agreement should specify the payment terms, including the amount of the sponsorship fee and the payment schedule.
- The dispute resolution mechanism: The agreement should specify the dispute resolution mechanism in the event of a dispute between the OCA and the marketing and sponsorship partner.

Marketing and Sponsorship Partner Relationships

The OCA's marketing and sponsorship partner relationships should be managed in accordance with the OCA's policies and procedures. The relationships should be based on mutual respect and cooperation.

The OCA should provide its marketing and sponsorship partners with the following:

- Access to OCA events and properties: The OCA should provide its marketing and sponsorship partners with access to OCA events and properties, such as the Asian Games and the Asian Winter Games.

- Marketing and promotional support: The OCA should provide its marketing and sponsorship partners with marketing and promotional support, such as advertising space in OCA publications and on OCA websites.
- Brand exposure: The OCA should provide its marketing and sponsorship partners with brand exposure through OCA events and properties.
- Return on investment: The OCA should ensure that its marketing and sponsorship partners receive a return on their investment.

The OCA should expect the following from its marketing and sponsorship partners:

- Financial support: The OCA should expect its marketing and sponsorship partners to provide financial support for OCA events and properties.
- Marketing and promotional support: The OCA should expect its marketing and sponsorship partners to provide marketing and promotional support for OCA events and properties.
- Brand alignment: The OCA should expect its marketing and sponsorship partners to align their brands with the OCA's brand.
- Compliance with OCA policies and procedures: The OCA should expect its marketing and sponsorship partners to comply with OCA policies and procedures.

The Marketing and Sponsorship Department is committed to generating revenue for the OCA through the sale of marketing and sponsorship rights. The department is also committed to building strong relationships with the OCA's marketing and sponsorship partners.

Marketing Plan

The OCA's marketing plan should be a comprehensive document that outlines the OCA's marketing goals, objectives, strategies, and tactics. The marketing plan should be updated on an annual basis, or more frequently as needed.

The OCA's marketing goals should be aligned with the OCA's overall mission and vision. The OCA's marketing objectives should be specific, measurable, achievable, relevant, and time-bound. The OCA's marketing strategies should be the means by which the OCA will

achieve its marketing objectives. The OCA's marketing tactics should be the specific activities that the OCA will undertake to implement its marketing strategies.

Marketing Budget

The OCA's marketing budget should be aligned with the OCA's marketing plan and should be approved by the OCA's Executive Board. The marketing budget should be monitored on a regular basis to ensure that it is being spent in accordance with the OCA's goals and objectives.

The OCA's marketing budget should be allocated to the following areas:

- Marketing research
- Marketing communications
- Marketing events
- Marketing partnerships
- Marketing technology

Marketing Communications

The OCA's marketing communications plan should outline the OCA's target audience, marketing messages, and marketing channels. The marketing communications plan should be updated on an annual basis, or more frequently as needed.

The OCA's target audience is the group of people that the OCA is trying to reach with its marketing messages. The OCA's marketing messages are the words and images that the OCA uses to communicate its brand, products, or services to its target audience. The OCA's marketing channels are the means by which the OCA will deliver its marketing messages to its target audience.

Marketing Research

The OCA's marketing research should be conducted on a regular basis to ensure that the OCA is aware of its target audience's needs and wants. Marketing research can be used to identify new market opportunities, to understand the competition, and to measure the effectiveness of marketing campaigns.

Marketing Ethics

The OCA's marketing ethics should be aligned with the OCA's overall values and should be communicated to all marketing employees. The OCA's marketing ethics should be reviewed on a regular basis to ensure that they are still relevant and appropriate.

The OCA's marketing ethics should include the following principles:

1. Honesty and integrity
2. Fairness and respect
3. Responsibility and accountability
4. Transparency and accountability
5. Sustainability

Procedures

Marketing and Sponsorship Strategy

1. Identify your target audience. The first step in developing a marketing and sponsorship strategy is to identify your target audience. Who are you trying to reach with your marketing and sponsorship efforts? Once you know your target audience, you can develop marketing messages and strategies that are relevant to them.

- Conduct market research to identify your target audience.
- Analyze the data from your market research to identify your target audience's needs and wants.
- Develop marketing messages and strategies that are relevant to your target audience.
- Develop marketing messages. Your marketing messages should be clear, concise, and persuasive. They should communicate the benefits of your products or services to your target audience.
- Write clear and concise marketing messages that are easy to understand.
- Use persuasive language that will convince your target audience to take action.
- Highlight the benefits of your products or services.

2. Select marketing channels. The channels you choose to use for your marketing and sponsorship efforts will depend on your target audience and your budget. Some common marketing channels include print, television, digital, and social media.

- Consider your target audience when selecting marketing channels.
- Choose marketing channels that are appropriate for your budget.
- Track the results of your marketing efforts to see which channels are most effective.

3. Allocate a budget. It's important to allocate a budget for your marketing and sponsorship efforts. This will help you track your progress and ensure that you're getting a return on your investment.

- Set a budget for your marketing and sponsorship efforts.
- Track your spending to ensure that you're staying on budget.
- Make adjustments to your budget as needed.

4. Identify sponsorship opportunities. There are many different sponsorship opportunities available, so it's important to identify those that are a good fit for your organization. Some common sponsorship opportunities include naming rights, event sponsorship, and product placement.

- Research different sponsorship opportunities.
- Identify sponsorship opportunities that are a good fit for your organization.
- Contact potential sponsors to inquire about their interest in sponsoring your organization.

5. Establish criteria for evaluating potential sponsorship partners. Once you've identified potential sponsorship partners, you need to establish criteria for evaluating them. Some factors to consider include the partner's financial resources, brand alignment, and commitment to your organization.

- Develop a list of criteria for evaluating potential sponsorship partners.
- Evaluate potential sponsorship partners against your criteria.
- Select the sponsorship partners that best meet your criteria.

Marketing and Sponsorship Agreements

1. Develop a draft sponsorship agreement. The draft sponsorship agreement should include the following elements:
    - The parties to the agreement
    - The term of the agreement
    - The scope of the agreement
    - The rights and obligations of the parties
    - The payment terms
    - The dispute resolution mechanism
2. Have the Procurement & Contract Manager review the draft sponsorship agreement. It's important to have a Procurement & Contract Manager review the draft sponsorship agreement to ensure that it is legally sound.

3. Negotiate the sponsorship agreement with the potential sponsor. The OCA Marketing and Sponsorship department should negotiate the sponsorship agreement with the potential sponsor to ensure that the agreement meets the needs of both parties.

4. Sign the sponsorship agreement. Once the sponsorship agreement has been negotiated, it should be signed by authorized representatives of the OCA and the potential sponsor.

5. Track the results of the sponsorship agreement. It's important to track the results of the sponsorship agreement to ensure that it is meeting the expectations of both parties.

6. Make adjustments to the sponsorship agreement as needed. If the sponsorship agreement is not meeting the expectations of either party, it may be necessary to make adjustments to the agreement.

By following these procedures, the OCA Marketing and Sponsorship department can ensure that marketing and sponsorship agreements are developed, negotiated, and executed in a way that protects the interests of the OCA and its sponsors.

Here are some additional tips for developing and negotiating marketing and sponsorship agreements:

- Be clear and concise in your writing.
- Use plain language that is easy to understand.
- Avoid jargon and technical terms.
- Be specific in your terms and conditions.
- Leave nothing to interpretation.
- Be prepared to negotiate.
- Be willing to compromise.
- Be flexible.
- Be professional.
- Build relationships.
- Trust your gut.
- Don't be afraid to walk away from a deal that isn't right for you.

Marketing and Sponsorship Partner Relationships

1. Establish clear expectations. It's important to establish clear expectations with your marketing and sponsorship partners at the outset of the relationship. This includes expectations about the level of service that you will provide, the level of involvement that you expect from your partners, and the desired outcomes of the relationship.

2. Communicate regularly. It's important to communicate regularly with your marketing and sponsorship partners throughout the course of the relationship. This will help to ensure that everyone is on the same page and that any potential problems can be addressed promptly.

3. Provide support. Your marketing and sponsorship partners are investing in your organization, so it's important to provide them with the support they need to be successful. This may include providing them with access to your events and properties, marketing and promotional support, or other resources.

4. Track results. It's important to track the results of your marketing and sponsorship partnerships to ensure that they are meeting your expectations. This will help you to make adjustments to the partnerships as needed.

By following these procedures, the OCA Marketing and Sponsorship department can ensure that marketing and sponsorship partner relationships are managed in a way that is beneficial to both the OCA and its partners.

Here are some additional tips for managing marketing and sponsorship partner relationships:

- Be responsive.
- Be proactive.
- Be flexible.
- Be honest.
- Be transparent.
- Be grateful.
- Be a good partner.

Marketing Plan Development

The marketing plan development process should include the following steps:

1. Define your goals and objectives. What do you want to achieve with your marketing plan? Do you want to increase brand awareness, generate leads, or drive sales? Once you know your goals, you can develop strategies to achieve them.

2. Understand your target audience. Who are you trying to reach with your marketing plan? What are their needs and wants? Once you understand your target audience, you can develop marketing messages and strategies that are relevant to them.

3. Set a budget. How much money do you have to spend on marketing? Once you know your budget, you can develop a marketing plan that fits your needs.

4. Choose the right marketing channels. Where will you reach your target audience? There are many different marketing channels available, so it's important to choose the ones that are most effective for your target audience and your budget.

5. Create marketing messages. What do you want to say to your target audience? Your marketing messages should be clear, concise, and persuasive.

6. Develop marketing materials. What marketing materials will you use to reach your target audience? This could include print materials, digital materials, or events.

7. Implement your marketing plan. Once you have developed your marketing plan, it's time to implement it. This means putting your plan into action and tracking your results.

8. Measure your results. How well is your marketing plan working? It's important to measure your results so you can see what's working and what's not. This will help you to make adjustments to your plan as needed.

9. Make adjustments as needed. Your marketing plan is not set in stone. As you learn more about your target audience and your competition, you may need to make adjustments to your plan. This is perfectly normal.

Marketing Budget Management

The marketing budget management process should include the following steps:

1. Set a budget. The first step in managing your marketing budget is to set a budget. This will help you track your spending and ensure that you're not overspending.

2. Track your spending. Once you've set a budget, it's important to track your spending. This will help you to see where your money is going and make adjustments as needed.

3. Allocate your budget. Once you've tracked your spending, it's time to allocate your budget. This means deciding how much money you're going to spend on each marketing activity.

4. Review your budget regularly. It's important to review your budget regularly. This will help you to make adjustments to your budget as needed, such as if your marketing goals change or your budget changes.

5. Make adjustments as needed. If you find that you're overspending, it's important to make adjustments to your budget. This could mean cutting back on certain marketing activities or finding ways to save money.

Marketing Communications Execution

The marketing communications execution process should include the following steps:

1. Plan your marketing communications. This includes defining your goals, target audience, and budget.

2. Create your marketing materials. This could include anything from brochures and flyers to social media posts and email campaigns.
3. Distribute your marketing materials. This could include sending them out via email, posting them on social media, or placing them in public places.
4. Create a marketing calendar. This will help you to plan your marketing activities and ensure that you're reaching your target audience with the right message at the right time.
5. Use a marketing automation platform. This can help you to automate your marketing tasks and save time.
6. Work with a marketing agency. If you don't have the time or resources to do your own marketing, you can work with a marketing agency to help you.
7. Track your results. This will help you see what's working and what's not so you can make adjustments as needed.

Here are some additional tips for executing marketing communications:

- Be clear and concise in your messaging.
- Use visuals to grab attention.
- Make it easy for people to take action.
- Track your results so you can see what's working and what's not.
- Make adjustments as needed.

Marketing Research

The marketing research process should include the following steps:

1. Define the research objectives

The first step in any marketing research project is to define the research objectives. This means clearly stating what you hope to achieve with the research. For example, you might want to:

- Understand your target market better
- Identify new market opportunities
- Evaluate the effectiveness of your marketing campaigns
- Develop new marketing strategies

Once you have defined your research objectives, you can begin to develop a research plan.

2. Develop a research plan

The research plan is a document that outlines the steps you will take to conduct your research. It should include the following information:

- The research methods you will use
- The sample size you will need
- The data collection methods you will use
- The data analysis methods you will use
- The timeline for the research project

3. Collect the data

Once you have developed a research plan, you can begin to collect the data. There are a variety of data collection methods available, including:

- Surveys
- Interviews
- Focus groups
- Observations
- Secondary research

The data collection method you choose will depend on your research objectives and the resources available to you.

4. Analyze the data

Once you have collected the data, you need to analyze it. This involves using statistical methods to identify patterns and trends in the data. The data analysis methods you use will depend on the type of data you have collected and the research questions you are trying to answer.

5. Report the findings

The final step in the marketing research process is to report the findings. This means writing a report that summarizes the research objectives, the research methods, the data collection methods, the data analysis methods, the findings, and the conclusions.

The report should be written in a clear and concise manner that is easy for the reader to understand. It should also be free of jargon and technical language.

Here are some additional tips for conducting effective marketing research:

- Use a variety of data collection methods. This will help you to get a more comprehensive view of your target market.
- Analyze the data carefully. This will help you to identify the key trends and patterns in the data.
- Report the findings clearly and concisely. This will help the reader to understand the results of your research.
- Use the findings to improve your marketing campaigns. This will help you to achieve your marketing objectives.

Marketing Ethics

The marketing ethics process should include the following steps:

1. Define the ethical guidelines

   The first step is to define the ethical guidelines that will be used to guide marketing activities. These guidelines should be based on the organization's core values and should be designed to protect the interests of all stakeholders, including consumers, employees, shareholders, and the community.

2. Create a code of ethics

   The ethical guidelines should be formalized in a code of ethics. The code of ethics should be clear, concise, and easy to understand. It should also be accessible to all employees, so that they are aware of the organization's expectations.

3. Incorporate the code of ethics into training

   The code of ethics should be incorporated into employee training programs. This will help to ensure that all employees are aware of the organization's expectations and that they are able to make ethical decisions in the workplace.

4. Create a system for reporting ethical violations

   The organization should create a system for reporting ethical violations. This system should be confidential and easy to use. Employees should feel comfortable reporting ethical violations, knowing that they will be taken seriously.

5. Investigate and take action on ethical violations

   All ethical violations should be investigated promptly and thoroughly. If an ethical violation is found, the organization should take appropriate action to address the issue. This may include disciplinary action, restitution, or termination of employment.

6. Promote ethical behavior

   The organization should promote ethical behavior throughout the organization. This can be done through employee training, communication, and by setting a good example from the top.

Accounting Policies and Procedures

Accounting Concept and Principles

Basic concepts of accounting

Financial accounting is the process of recording, classifying, and summarizing, in quantitative terms, the economic events of a business. The result of this process is a compilation of information which reports the financial position of a business at a certain point in time and the results of its operations during a period of time. A basic objective of financial statements is to provide reliable and relevant financial information for the evaluation of a business.

The accounting process records the economic events of an OCA by making additions to and removals from specific classifications known as accounts. There are five general types of accounts: assets, liabilities, net position, revenues, and expenditures.

Assets are economic resources over which an organization has control and ownership. Examples of these include cash, claims to receive cash (accounts receivable), buildings, land, equipment, etc. Liabilities are economic obligations of the OCA such as taxes, outstanding bills (accounts payable), leases, and other debts. Net position represents the excess of assets of an organization over its liabilities.

The two remaining categories of accounts, revenues and expenditures, are used to record the inflows and outflows of financial resources of OCA during a specific period of time.

Total revenues over expenditures are compared at the end of each accounting period (usually months) and the excess of revenues over expenditures is accumulated throughout the fiscal year. This amount is referred to as the Change in Net Position. At the end of the fiscal year, this amount will be combined with the Net Position for the organization and the total Net Position will be carried forward to the next fiscal year. Likewise, if expenditures exceed revenues, then a reduction to the Net Position is recorded.

Fiscal year

OCA has adopted the calendar year which begins on 1st of Jan and ends on 31st of Dec as its fiscal year.

Administrative controls

Administrative controls are primarily designed to promote operational efficiency and adherence to managerial policies. Administrative controls include the plan of Organization, the procedures and records concerned with the decision-making process, the operational efficiencies of OCA and the quality control considerations of services rendered.

Communication of financial and service objectives to all staff is inherent in effective administration.

Strong internal controls require that the Organization's structure be formally established with clearly defined areas of responsibility and authority. This formal plan should be in writing and include such items as organizational charts, job descriptions, and internal policy manuals.

Benefits of an Accounting Manual

The accounting policies and procedures manual offers central benefits, prominently among them being cost savings. Clearly defined policies outline precise processes, designate responsible parties, and emphasize asset protection. This clarity alleviates the need for administrators to consistently seek management direction for specific transactions, streamlining operations and contributing to overall cost effectiveness. The central benefit with an accounting policies and procedures manual is cost savings.
Policies that clearly articulate the process to be followed, who should carry out the action, and the safeguarding of the assets save an administrator from having to seek management direction on a particular transaction.

An accounting policy manual limits the time that has to be spent by management on internal discussions each time a transaction for which no specific policy is clearly stated appears.

An accounting policy approval process stated in the manual gives management formal control over who can determine accounting policy. The formal control also gives management an opportunity to assure that the policies conform the Financial Accounting Standards Board (FASB) recommendations.

Management has an opportunity to improve current accounting policies and procedures while reviewing the accounting system in the organization.

Auditors are able to assess the organization’s accounting control and procedures in an easy way by reading the accounting policy manual. Transactions that do not comply with policy are thereby easier to detect. Documented policies that are adhered to should reduce the number of tests of control that an auditor will undertake during an audit, which may result in savings.

Policy Development

Consider the importance of senior management support

- Accounting policies and procedures should be actively supported by an appropriate level of management to emphasize their importance and authority. Management's support for the manual is essential for its actual impact and legitimacy in the organization.

Plan for periodic reviews and updates

- The documentation of accounting policies and procedures should be reviewed periodically according to a predetermined schedule and updated if needed. Changes in policies and procedures that occur between these periodic reviews should be updated in the documentation promptly as they occur. Each policy should have its own specific date for review.

Assign an employee to oversee the process

- A specific employee should be assigned the duty of overseeing the documentation process. The employee will be overseeing the accounting policy process and the writing of the policy manual. Adequate knowledge and effective communication with managers in the organization are necessary for the function. It is management's responsibility for ensuring that this duty is performed consistently.

Make the policies and procedures readily available

- The documentation of accounting policies and procedures should be readily available to all employees who need it.

Clarify employees' responsibilities

- The documentation of accounting policies and procedures should indicate which employees are to perform which procedures, especially who has the authority to authorize transactions and the responsibility for the safekeeping of assets and records.

Document the actual procedures

- Procedures should be described as they are intended to be performed rather than in some idealized form. The acceptance of the manual by management can be poor if the accounting policies and procedure are changed radically.

Clearly state the purpose of the policies

- The documentation of accounting policies and procedures should explain the design and purpose of control-related procedures to increase employee understanding of and support for controls. This can be done in the introduction of the manual and as a short explanation for each policy statement.

Create and communicate a policy approval procedure

- An accounting policy approval procedure should be created and communicated throughout the organization. This process can be formal or informal but should not be burdensome to the degree that managers do not raise issues that need to be addressed by the assigned employee. The process for approval should be documented in the accounting policy manual.

Accounting Responsibilities

The following is a list of personnel who have fiscal and accounting responsibilities:

Finance Committee

- Approves the yearly budget forecast prepared by the Finance Director/Chief Finance Officer (CFO)
- Advises on raising funds to ensure the Council's independence
- Approves the audited statements of accounts and submits them to the Executive Board and General Assembly for ratification and further approvals.
- Reviews and approves internal controls and accounting policies and procedures
- Approves and contracts with the auditors

President

- Supervising the preparation of the financial, administrative and other reports and submits them to the Executive Board after approval of Finance Committee's report and audited financial statements of the Council for consideration and presents them before the General Assembly.
- Signing Host City Contracts for Asian Games
- Signing any agreements / contracts.
- Signing banking transactions up to USD2 million solely; above USD2 million jointly with CEO/Director General or one member of the Finance Department
- Supervising the yearly budget forecast prepared by OCA Finance Director/Chief Finance Officer (CFO)

CEO/Director General

- Shall be in charge of the day-to-day financial operation of the OCA headquarters, Museum, Academy and Conference Hall.
- Signing any agreements / contracts.
- The CEO/Director General of OCA is authorized to sign payments up to USD1 million solely. Payments above USD1 million shall be signed jointly by the CEO/Director General of OCA and a member of the Finance Department (as assigned by the CEO/Director General).
- Approving day-to-day financial expenditure of OCA including cash payments
- Appointing and dismissal of OCA staff
- Signing the employment contract of OCA staff
- Signing any legal agreement and approving its cost
- Execute the OCA development program.
- Opening and operating OCA Bank accounts including bank transfers, cheque payments. This includes opening operating bank accounts in any location and currency.
- Appointment of short term and long-term consultancy agreements (agreement can be verbally or written form)
- Approve the list of participants for various OCA events including the invited guests
- Shall be responsible to make bank transfers/transactions to the benefit of Olympic Movement and other relevant agencies on, an as and when required basis
- Will keep records of the OCA revenues and expenditure.
- Will be responsible for OCA promotions, activities, marketing and others
- Taking any action to protect the property and financial interest of OCA
- Will pay all contractual obligation of the OCA.
- Will report to the President as well as to the external auditors showing full accounts of the Council

- Will be responsible for all financial transaction of the Council during all official missions at HQ or abroad.
- Signing the financial guidelines and governance after approving by OCA Finance Committee and executive board
- Will be responsible to hire office equipment and space, if need be, inside or outside Kuwait, and cover remuneration/expenses as per local laws.
- Will be responsible to hire international staff for special OCA missions and pay their air ticket, accommodation and indemnity of USD 100/- per day with a minimum of US $ 300 per mission and agreement fee if any
- Taking any decision related to paying bonus, special incentive or overtime
- Will maintain record of the special OCA development fund related to OCA Olympic Movement
- Will assume separate financial management and audit of the Olympic Solidarity programs and may adopt measures of payment according to the prescribed procedures.
- In case Finance Director/Chief Finance Officer (CFO) cannot fulfil his duties, the President of OCA will appoint a member from the OCA Finance Department to carry out Finance Director/Chief Finance Officer (CFO)'s duty concerning financial affairs till Finance Director/Chief Finance Officer (CFO) resumes his / her duties or new Finance Director/Chief Finance Officer (CFO)'s appointment.
- The Finance Director/Chief Finance Officer (CFO) shall assign some of his financial responsibilities to other members from OCA Finance Department as deemed fit.

Finance Director/Chief Finance Officer (CFO)

- Coordinate and support the CEO/Director General in formulating the Financial Strategies and Framework for OCA.
- Prepare annual forecast budget in Coordination with CEO/Director General
- Overall supervision of the Finance Department.
- Review and verification of accounting transactions.
- CEO/Director General with the Internal Auditor to execute Internal Audit works.
- CEO/Director General with the External Auditors for the issuance of Annual Financial Statements
- Submission of Annual Internal and External Audit Reports to the OCA CEO/Director General, Finance Committee, Executive Board and General Assembly for approval.
- The Finance Director/Chief Finance Officer (CFO) of OCA is authorized to sign payments up to USD15,000 / KWD5,000, solely. Payments above USD15,000 / KWD5,000 up to USD100,000 / KWD30,000 shall be signed jointly with another member of the Finance Department or the CEO/Director General.

Financial Officer

- Keep proper documentation of each financial transaction
- Verification & authentication of all vouchers, bills and receipts for petty expenses provided by relevant staff
- The Finance Officer of OCA is authorized to sign payments up to USD15,000 / KWD5,000, solely. Payments above USD15,000 / KWD5,000 up to USD100,000 / KWD30,000 shall be signed jointly with another member of the Finance Department (as assigned by the CEO/Director General).
- Payment of petty expenses subject to approval of Finance Director/Chief Finance Officer (CFO)
- Accepting the invoices from local vendors & verification of its authentication and report to Finance Director/Chief Finance Officer (CFO)

- Prepare local and international bank transfers
- Intimate the payment status to vendors / beneficiary with copy of bank transfer, if possible
- Viewing rights of OCA Bank accounts without any transaction rights
- Verbal communication with Banks, on behalf of Finance Director/Chief Finance Officer (CFO), for any clarification on payment transfers
- Monitor cash flows within various OCA accounts and prepare bank letters for maintaining the accounts with enough fund
- Monthly reconciliation of cheques, its payment status
- Preparation of staff's salary
- Verify the NOC activities report and report to Finance Director/Chief Finance Officer (CFO)
- CEO/Director General with NOCs for shortfalls if any on the activities report
- Prepare the payment letters favoring to NOC activities and other rightful payment to Olympic Movement in Asia
- Intimate the payment info to NOCs with documentary proof if possible
- Communicate with NOCs, AFs, NFs, IFs and OCA Standing Committee Members for OCA meetings air travel / airfare
- Communicate with OCA EB Members, Asian IOC Members, AFs, IFs, invited guests for OCA meetings air travel / airfare
- Economy class cash reimbursement of airfare for OCA Standing Committee Members attending meetings and per diem of USD 300 per meeting
- Business class cash reimbursement of airfare for OCA EB Members attending meetings and per diem as per OCA Rules
- Economy class cash reimbursement of airfare for one participant per NOC attending OCA General Assembly
- Invoices: preparing the invoices for IT and TV Audits, dispatching, book keeping and close monitoring of its payments from Asian Games Organizing Committees

- Prepare the invoices for Asian Games Organizing Committee and TV Rights Host Broadcasters, dispatching, book keeping and close follow-up for its payments
- Responsible for keeping all financial documents of OCA meetings together with receipt, invoice / copy of air ticket / air travel and other supporting documents
- Responsible to handover all financial transactions to Internal Auditor on monthly basis together with all relevant supporting document

Chart of Accounts

Chart of Accounts

The Chart of Accounts is the framework for the general ledger system and the basis for the accounting system. The Chart of Accounts consists of account titles and account numbers assigned to the titles.

OCA has designated a Chart of Accounts specific to its operational needs and the needs of its financial statements.

To facilitate the record keeping process for accounting, all ledger accounts are assigned a descriptive account title and account number. The Chart of Accounts is structured so that financial statements can be shown by natural classification (expense type) as well as by functional classification.

The Finance Director/Chief Finance Officer (CFO) is responsible for maintaining the Chart of Accounts and revising as necessary.

General Ledger

The general ledger is the collection of all asset, liability, net assets, revenue and expense accounts. It is used to accumulate all financial transactions and is supported by subsidiary ledgers that provide details for certain accounts. The general ledger is the foundation for the accumulation of data and production of reports. The accounting department is responsible for the proper posting of journals and entries to the general ledger and for the maintenance of the accounts to ensure accuracy, validity and reliability of financial records.

All input and balance are the responsibility of the Finance Officer with final approval by the Finance Director/Chief Finance Officer (CFO).

The Finance Director/Chief Finance Officer (CFO) should review the General Ledger on a periodic basis for any unusual transactions.

Design of Accounts

Accounts have titles and numbers that indicate specific ledger accounts such as banking account, account receivable, accounts payable etc.

Accounts are arranged in the same sequence in which they appear in the financial statements, that is, asset accounts should be numbered first, followed by liability accounts, owner's equity accounts, revenue accounts and expense accounts as follows:

- 100 - 199 Asset Accounts
- 200 - 299 Liability Accounts
- 300 - Net Positions
- 400 - 499 Revenue Accounts
- 500 - 599 Expenditures Accounts

A sub-division among the balance sheet accounts is also designated by short term to long term, (i.e. current assets precede long term assets and current debt precedes long-term debt accounts).

Further, accounts are numbered so that expense amounts are recorded according to the department that is accountable for the cost and the nature of the cost.

Unassigned number sequences should be left open within each group of accounts to provide for additional accounts which may be added later.

Assets

Assets are probable future economic benefits obtained or controlled by the Organization as a result of past transactions or events. Assets are classified as current assets, fixed assets, contra-assets, and other assets.

- **Current assets** are assets that are available or can be made readily available to meet the cost of operations or to pay current liabilities. Some examples are cash, temporary investments, and receivables that will be collected within one year of the statement of financial position date.
- **Fixed assets** (property and equipment) are tangible assets with a useful life of more than one year that are acquired for use in the operation of the Organization and are not held for resale.
- **Contra-assets** are accounts that reduce asset accounts, such as accumulated depreciation and reserves for uncollectible accounts receivable.
- **Other assets** include long-term assets that are assets acquired without the intention of disposing them in the near future. Some examples are security deposits, property and long-term investments.

Liabilities

Liabilities are probable future sacrifices of economic benefits arising from present obligations of the Organization to transfer assets or provide services to other entities in the future as a result of past transactions or events. Liabilities are classified as current or long term.

- **Current liabilities** are probable sacrifices of economic benefits that will likely occur within one year of the date of the financial statements or which have a due date of one year or less. Common examples of current liabilities include accounts payable, accrued liabilities, short-term notes payable, and deferred revenue.

- **Long-Term Liabilities** are probable sacrifices of economic benefits that will likely occur more than one year from the date of the financial statements. An example is the non-current portion of a mortgage loan.

Net position

Net Position is the difference between total assets and total liabilities.

Revenues

Revenues are inflows or other enhancements of assets, or settlements of liabilities, from Sponsorships, Broadcasting rights, Ticket sales, Licensing and merchandising, Government funding, Donations and contributions or other activities that constitute an organization’s ongoing major or central operations.

Expenditures

Expenditures are outflows or other activities using assets, or incurrences of liabilities from Sponsorships, Broadcasting rights, Ticket sales, Licensing and merchandising, Government funding, Donations and contributions or other activities that constitute an organization’s ongoing major or central operations, or carrying out other activities that constitute OCA ongoing major operations.

Transactions in the General Ledger

All activities recorded in journals will be posted to the general ledger using the computerized posting feature. These journals include:

- Cash Journal
- Revenue Journal
- Expenditure Journal

Posting transactions

Recurring journal entries will be established for adjustments that occur equally each monthly accounting period. Recurring journal entries can include the following:

- Amortization of prepaid expenses
- Depreciation of Fixed Assets

Recurring journal entries are reviewed monthly and adjusted accordingly.

Adjusting journal entries are prepared for transactions that have not been recorded in other journals or to correctly restate account balances to accurate amounts. The need to make adjusting journal entries may be due to any of the following:

- Accrual of income and expense items
- Correction of errors
- Recording of non-cash transactions

All journal entries are reviewed and authorized by the Financial Officer before being posted. Adequate supporting documentation will be prepared and maintained for each journal entry.

Journal Entries

All journal entries to the organization's general ledger must be properly prepared, documented, reviewed, approved, recorded and maintained in accordance with GAAP.

- All journal entries are to be signed by both the Financial Officer and Finance Director/Chief Finance Officer (CFO) prior to posting.
- Person(s) preparing a journal entry cannot approve the same journal entry.
- All journal entries should have supported documentation and a description that fully explains the nature of the entry and amounts being recorded.
- All journal entries have to be properly processed prior to closing the accounting period.
- All posted journal entries and related documentation should be maintained in an accessible file for review by management and external auditors, if necessary.

Cash Disbursements

Cash payments are generally made for the payment of services or for reimbursement. They may also be paid by cheque.
Cheques are processed regularly. Invoices submitted to the accounts payable department as and when received and are processed and paid.

Disbursement requests are submitted to accounting in three ways:

Original invoice

Purchase requisition (submitted on an approved form)

Employee expense report or reimbursement claim

All invoices must have the account code written and approved by the department supervisor before being submitted to accounting.

Each employee's claim for reimbursement or purchase must be documented on the approved form with the travel authorization, receipts, the nature of the activity and the source of funding (if applicable) before being approved for reimbursement as follows:

Accommodation: An itemized receipt from the hotel detailing all expenses, the person(s) for whom the accommodation was provided and the specific business purpose

Meals and entertainment: A receipt must be provided showing the cost of food, beverages and gratuities, including the name of each person for whom the food or beverage was provided and the specific business purpose.

Other expenses: A receipt from the vendor detailing all goods or services purchased (including the category of service for transportation) and the specific business purpose.

The Financial Officer reviews all claims for payment and:

Verifies the expense and the amount

Approves the payment if it is in accordance with the budget

Provides or verifies appropriate information on the allocations

Provides the payment date taking into account cash flow projections

Submits to the Bookkeeper for processing

The accountant processes all payments and:

Enters them immediately in the Accounts Payable module;

Prints checks according to the allocation and payment date provided by the Financial Officer;

Submits the checks, with attached backup documents, to the Finance Director/Chief Finance Officer (CFO) for approval and signature;

The Finance Officer of OCA is authorized to sign payments up to USD15,000 / KWD5,000, solely. Payments above USD15,000 / KWD5,000 up to USD100,000 / KWD30,000 shall be signed jointly with another member of the Finance Department (as assigned by the CEO/Director General).

The Finance Director/Chief Finance Officer (CFO) of OCA is authorized to sign payments up to USD15,000 / KWD5,000, solely. Payments above USD15,000 / KWD5,000 up to USD100,000 / KWD30,000 shall be signed jointly with another member of the Finance Department or the CEO/Director General.

The CEO/Director General of OCA is authorized to sign payments up to USD1 million solely. Payments above USD1 million shall be signed jointly by the CEO/Director General of OCA and a member of the Finance Department (as assigned by the CEO/Director General).

Signing banking transactions up to USD2 million solely; above USD2 million jointly with CEO/Director General or one member of the Finance Department.

Stamp invoice "Paid";

Send checks and appropriate backup documents;

File all backup documents in the appropriate folder;

Establishes an accounts payable aging at the middle and end of each month and submits to the Finance Director/Chief Finance Officer (CFO) to ensure the timely payment of all invoices.

Bank Reconciliation

Bank reconciliation shall be made monthly within 30 days of the date of receipt of bank statements. Upon receipt of the monthly bank statement including cleared checks, deposit slips and any other transaction notifications, the monthly bank reconciliation is prepared by the accountant and reviewed by the Finance Director/Chief Finance Officer (CFO).

All cleared transactions on the bank statement will be reconciled and cleared in the accounting system. After all cleared items for the month have been selected, the book ending balance and the bank ending balance must match with a zero difference.

A printed copy of the completed detail reconciliation must be attached to the appropriate original bank statement each month.

Any discrepancies between these two balances will require research to determine the cause, such as recording errors, omissions, mis postings, etc. This may also include recalculation of the bank statement for any possible errors made by the bank.

Bank reconciliation should be done as follows:

- All bank statements are given unopened to the Finance Director/Chief Finance Officer (CFO). The Finance Director/Chief Finance Officer (CFO) reviews the statements for unusual balances and/or transactions.
- The Finance Director/Chief Finance Officer (CFO) gives the statements to the Finance Officer for timely reconciliation as follows:
    - A comparison of dates and amounts of deposits as shown in the accounting system and on the statement,
    - A comparison of inter-account transfers, an investigation of any rejected items, a comparison of cleared checks with the accounting record including amount, payee, and sequential check numbers.

- The Finance Officer will verify that voided checks, if returned, are appropriately defaced and filed.
- The Finance Officer will investigate any checks that are outstanding over six months.
- Any book reconciling items such as interest, bank charges and any recording errors are summarized and drafted in journal entry form for recording to the general ledger. All supporting documentation will be maintained for audit purposes.
- The Finance Officer will attach the completed bank reconciliation to the applicable bank statement, along with all documentation.
- The reconciliation report will be reviewed, approved, dated, and initialed by the Finance Director/Chief Finance Officer (CFO).

Account Receivable

Recognition

Under the cash basis, revenues are recognized only when cash is received and deposited into a revenue account(s). Cash-based systems do not interface with OCA's automated accounts receivable system.

Under the accrual method, revenues are recognized and credited to a revenue account(s) when invoices are processed through the automated accounts receivable system.

Accounting entries

- The Finance Officer will create all journal entries for accounts receivable and prepare them based on month-end billing information. The Finance Director/Chief Finance Officer (CFO) reviews and approves all accounts receivable journal entries.
- After approval, the Finance Officer records the entries. In the absence of the Finance Officer, the Finance Director/Chief Finance Officer (CFO) will prepare the entry and the Controller will review, approve and record the entry.
- Each month, the Finance Officer shall prepare an aging report of individual billing information and days overdue, which he shall then forward to the Finance Director/Chief Finance Officer (CFO) for review. This report shall be provided to management on a monthly basis.
- The Finance Officer shall record payments in the general ledger from which are deposited directly into the organization's bank account and apply the funds to outstanding invoices.
- The Finance Officer is responsible for reconciling receipts from funding sources with accounts receivable and for issuing credit notes to the accounts upon receipt of the money and notification by the Billing Officer that unauthorized costs will not be resubmitted for payment. The Finance Director/Chief Finance Officer (CFO) review, approve, and post the credit memo entries

Account Payable

Documentation for account payable

The following documents are forwarded to accounting department for temporary filing and subsequent matching to form an accounts payable voucher package:

- Purchase Order if applicable
- Vendor invoice
- Packing slip
- Check request with proper approvals if applicable

Once the accounting department has all of the above documents, the following steps are performed to ensure proper authorization, validity of purchase, receipt of purchased items or services and accuracy of amounts.

- The vendor invoice will be attached to the check request. When applicable, the purchase order should also be attached along with any other supporting documentation.
- The purchase order should be evaluated for proper authorization and the nature of the purchase and pricing as shown on the invoice reviewed for validity.
- The quantities shown shipped or delivered on the invoice will be compared to the packing slip.
- Calculations on the invoice will be recomputed, such as, quantities received multiplied by unit price and totals. Sales tax amounts listed on the invoice will be reviewed so that when appropriate, sales tax-exempt notifications can be sent to the vendor.

- If any paperwork needs to be mailed with the account payable check, the department forwarding the request needs to send the original and a copy of the document that must accompany payment.
- Any discrepancies to the steps listed above must be addressed and resolved prior to commencing with the accounts payable voucher. If necessary, requests will be returned to requestor for necessary corrections.

Recording

Once the set of vouchers has been correctly assembled, it is then reviewed by the accounting department to ensure that it is correctly coded and accurate. Once this review is completed, it is then entered into the OCA's accounting software.

Payment of account payable

Every week, accounts payable invoices are selected for payment according to their terms for payment. Accounts payable should normally be paid within 7 days of their due date unless otherwise determined by the accountant. If payment terms are not specified on the invoice, payment will be issued within 30 days of the invoice date.

Any debit balances (amounts owed) are applied to credit amounts when determining payment.

Accounts payable invoices are submitted to the Finance Director/Chief Finance Officer (CFO) for review and payment approval. Upon approval, checks are then printed for the accounts payable invoices to be paid.

After the checks are printed, they are matched to the voucher package and submitted to an authorized signatory as per approved limits.

Upon return of the checks to accounts payable, the 2-part checks will be separated and processed as follows:

Payroll Administration

Payroll Administration

OCA operates on a monthly payroll. The objectives of the following payroll procedures are to ensure:

- A timely and efficient processing of the staff payroll.
- An accurate computation and recording of payroll expense, related liabilities, and net pay.
- Payment for only authorized work actually performed.

Preparation of Timesheets

Each employee is required to submit an electronic timesheet no later than on the Last Working Day of the month (each pay period) using the fingerprint system. Timesheets shall adhere to the following guidelines:

- Timesheets submitted electronically via the fingerprint system will be considered as signed by the employee, affirming the accuracy of the information.
- Every timesheet must accurately reflect all hours worked during the respective pay period.
- Any errors identified should be rectified electronically, with notification provided to the Finance Director/Chief Finance Officer (CFO).
- Compensated absences (such as vacation, holiday, sick leave, etc.) must be

Processing of Timesheets

After all timesheets have been approved, the accountant reviews the timesheets to verify charge codes and work hours and then transfers time sheets to the accounting system.

Once the payroll is processed and calculated, the payroll reports are printed and reviewed/approved by the Finance Director/Chief Finance Officer (CFO). The direct deposit file is created after the payroll reports are approved. Employee leave accruals are calculated and posted.

The accountant creates the direct deposit file which shall be transmitted to the bank. Following the transmission of the direct deposit file, payroll is posted, ensuring accurate and timely financial processing.

Timesheet Corrections

If an employee needs to make a change or a correction to a timesheet, the employee must contact the Financial Officer with the detail information. The Financial Officer will make the change/correction to the timesheet. The accountant will use the detailed information provided to make the necessary journal entries for the timesheet correction. Each timesheet correction must include a reason as to why the change was needed and must be approved by the Financial Officer prior to posting.

Distribution of Payroll

Establish direct deposit for each employee through the organization's payroll system, as all employees are compensated through direct deposit. Cash payments shall be distributed by individuals who neither approve timesheets, have hiring or firing responsibilities, nor oversee the preparation of payroll.

Changes in Payroll Data

All of the following changes in payroll data are to be authorized in writing:

- New hires
- Terminations
- Changes in salaries and pay rates
- Voluntary payroll deductions
- Court-ordered payroll deductions

New hires, terminations, and changes in salaries or pay rates shall be authorized in writing by the appropriate Department Director / Head and the Finance Director/Chief Finance Officer (CFO).

Any changes that affect payroll processing will be forwarded to the accountant once they have been entered into the automated master file by Personnel.
The accountant will not have access to make changes to rates of pay or payroll deductions.
Documentation supporting any changes to the payroll status of an employee will be permanently maintained in the employee's personnel file.

To assure that changes are implemented accurately, the accountant will distribute a preliminary register to the HR Specialist for review and approval before posting the payroll and disbursing payments.

The Payroll Specialist will submit the recommendation for disbursement of the payroll direct deposits to the Finance Director/Chief Finance Officer (CFO) for approval and sent to the CEO/Director General for final approvals for the release of payment.

Property and Equipment

Capitalization Policy

Physical assets acquired with unit costs in excess of USD 5,000 are capitalized as fixed asset on OCA's general ledger. Items with unit costs below this threshold shall be expensed in the year purchased.

Capitalized property and equipment additions are recorded at their historical cost. All such assets, except land, undergo depreciation based on their estimated useful life. For Furniture and Fixtures (F&F) and Computers, the estimated useful life is 36 months, while for Vehicles, it is 48 months. The straight-line method of depreciation is employed, with no residual value at the end of the determined useful life.
Establishment and maintenance of fixed asset

- Date of acquisition
- Cost
- Description (including color, model, and serial or other identifying number)
- Funding source of the equipment (including percentage of Federal Participation)
- Location of asset
- Use and Condition of the equipment
- Date of Disposal/Sale Price.

All capitalized property and equipment shall be recorded in a property log. This log shall include the following information with respect to each asset:

A physical inventory of all assets capitalized under the preceding policies will be taken every five years by OCA. This physical inventory shall be reconciled to the property log and adjustments made as necessary.

Depreciation and useful lives

All capitalized assets are maintained in the special property and equipment account group and are not included as an operating expense.

In the year of acquisition, depreciation is recorded based on the number of months the asset is in service, counting the month of acquisition as a full month.

For accounting and interim financial reporting purposes, depreciation expense will be recorded on a monthly basis.

Repair of property and Equipment

Expenditures to repair capitalized assets shall be expensed as incurred if the repairs do not materially add to the value of the property or materially prolong the estimated useful life of the property.

Expenditures to repair capitalized assets shall be capitalized if the repairs increase the value of property, prolong its estimated useful life, or adapt it to a new or different use. Such capitalized repair costs shall be depreciated over the remaining estimated useful life of the property. If the repairs significantly extend the estimated useful life of the property, the original cost of the property shall also be depreciated over its new, extended useful life.

Dispositions of property and equipment

If equipment is sold, scrapped, donated or stolen, adjustments need to be made to the fixed asset listing and property log. If money is received for the asset, then the difference between the money received and the "book value" (purchase price less depreciation) of the asset will be recorded as a loss (if the money received is less than the book value) or a gain (if the money received is more than the book value).

Cash, Deposit & Transfer

Cash Receipts

Cash receipts generally come from contracts and provision of services. Accurate internal control of cash receipts and deposits must be maintained at all times. Cash deposits must be made within 24 hours of receipt.

The main steps in the collection procedure are as follows:

- The receptionist receives incoming mail and forwards it unopened to the Finance Director/Chief Finance Officer (CFO). The Finance Director/Chief Finance Officer (CFO) opens, dates and distributes the mail. The Finance Director/Chief Finance Officer (CFO) records all cheques in a logbook, stamps all cheques "for deposit only" and makes two (2) copies of each cheque. The cheques are kept in a locked cabinet until they are given to the bookkeeper for processing and deposit.
- Each week, the Finance Director/Chief Finance Officer (CFO) shall submit the following to the Finance Officer for processing: the endorsed cheques, the deposit register and the correct account allocation for each deposit. The Finance Officer processes the deposit and brings it to the bank for deposit. A copy of the deposit slip is attached to the deposit. Deposits are placed in a file to be attached to the bank statement. The deposit logbook is returned to the Finance Director/Chief Finance Officer (CFO).
- All cash received will be counted, verified and signed by the Finance Director/Chief Finance Officer (CFO) and another available staff member. The cash will be immediately accounted for using the appropriate allocation. A receipt will be given to the payer and a copy will be kept for internal purposes. The money will be kept in a locked and secure location and deposited within 24 business hours.

Petty Cash

To facilitate minor business expenses, a petty cash fund will be available to employees. The Finance Officer act as custodian of the petty cash fund.

To prevent access by anyone except the Finance Officer, petty cash must be kept in a locked strong box in a locked desk or cabinet whenever not in use or whenever the Finance Officer is absent.

When an employee requests a petty cash draw, the Finance Officer will record the amount advanced, date of disbursement, reason for the draw and name of the employee receiving the advance.

At the end of each month or whenever the petty cash fund drops below a balance of $1,000.00 (US Dollars One Thousand), the accountant completes the replenishment paperwork from the journal with the itemized descriptions of expenses and attaches all vouchers and submits to the Finance Director/Chief Finance Officer (CFO) for review and approval.

Deposit

The accountant prepares the deposit slips and make the deposits to the OCA’s authorized bank.

The final net cash deposit must reconcile with the original accounting department log.

Inter-bank transfer

The Financial Officer monitors the balances in the bank accounts to determine when there is a shortage or excess in the checking account. The Financial Officer recommends to the

Finance Director/Chief Finance Officer (CFO) when a transfer should be made to maximize the potential for earning interest. The accountant is directed in writing when to make a transfer and in what amount. A copy of the transfer is given to the Financial Officer.

Credit Card & Accrual

Credit Card & Charges

All staff members who are authorized to carry an organization credit card will be held personally responsible in the event that any charge is deemed personal or unauthorized. Unauthorized use of the credit card includes: personal expenditures of any kind; expenditures which have not been properly authorized; meals, entertainment, gifts, or other expenditures which are prohibited by budgets, laws, and regulations, and the entities from which OCA receives funds.

The receipts for all credit card charges will be given to the Finance Director/Chief Finance Officer (CFO) within two (2) weeks of the purchase along with proper documentation. The Finance Director/Chief Finance Officer (CFO) will verify all credit card charges with the monthly statements. A record of all charges will be given to the accountant with applicable allocation information for posting. A copy of all charges will be attached to the monthly credit card statement when submitted to the Finance Director/Chief Finance Officer (CFO) for approval and signing.

Accrual

To ensure a timely closure of the General Ledger, OCA may book accrual entries. Some accruals will be made as recurring entries.

Accruals to consider:

- Monthly interest earned on money market accounts, certificates of deposits, etc.
- Recurring expenses, including employee vacation accrual, prepaid corporate insurance,
- Depreciation, etc.

Month End Closing

Overview

OCA's fiscal year begins 1st of Jan and ends 31st Dec. OCA closes its books at the end of each calendar month.

The policies and procedures for closing the books on a monthly basis are included in this section; however, these procedures will not always apply at the end of the fiscal year.

Closing Process

The following closing process summarizes the monthly closing activities. Each month will be closed within 15 days from month end.

- Prepare and enter journal entries
- Prepare all cost allocation entries
- Revenue Recognition, i.e. revenues are earned as expenses are incurred. Interest income is accrued through the various investments.
- Preparation of monthly Financial Report
- Submit monthly Financial Report to Finance Director/Chief Finance Officer (CFO) for review and the President for approval.

Preparing financial statements and communicating key financial information is a necessary and critical accounting function.

Financial statements are management tools used in making decisions, in monitoring the achievement of financial objectives, and as a standard method for providing information to interested parties external to the Organization.

Financial statements may reflect year-to-year historical comparisons or current year budget to actual comparisons.

OCA prepares monthly reports that are distributed both internally and to the Board of Directors.

The monthly report is a Financial Status Report that reflects budget to actual comparisons of revenues and expenditures and changes. Included is a footnoted variance analysis that provides explanatory information on material differences between budget and actual.

Year End Closing and Annual Audit

Year End Closing

OCA closes the books on a fiscal year-end basis in connection with the annual audit. It is OCA's policy to perform all of the work necessary to close the books and compute the year-end balances for the annual audit. The goals of the closing are to:

- Identify material discrepancies
- Review accuracy of data
- Verify completeness of data
- Correct classification of data

During the closing process, the accounting department will notify each department of the deadlines for submitting any outstanding invoices or billings.

The reconciliation of balance sheet accounts and yearend financial reports will be prepared after the closing of accounts payable, accounts receivable and payroll.

Preparation for the annual audit

OCA shall be actively involved in planning for and assisting with the Organization's independent accounting firm in order to ensure a smooth and timely audit of its financial statements. In that regard, the Accounting Department shall provide assistance to the independent auditors in the following areas:

Planning: The Finance Director/Chief Finance Officer (CFO) is responsible for delegating the assignments and responsibilities to accounting staff in preparation for the audit.

The assignments shall be based on the list of requested schedules and information provided by the independent accounting firm.

Involvement: Organization staff will do as much work as possible in order to assist the auditors thereby reducing the cost of the audit.

All financial statements, schedules and footnotes will be prepared by the accounting department.

Throughout the audit process, OCA will make every effort to provide schedules, documents and information requested by the auditors in a timely manner.

Conclude the audit

OCA and the independent auditor will review the draft of the financial statements, footnotes, and required audit letters consisting of the following procedures:

- Carefully read the entire report for typographical errors.
- Trace and agree each number in the financial statements and accompanying footnotes to the accounting records and/or internal financial statements of OCA.
- Review each footnote for accuracy and completeness.

Any questions or errors noted as part of this review shall be communicated to the independent auditor in a timely manner and resolved to the satisfaction of the Finance Director/Chief Finance Officer (CFO).

It shall also be the responsibility of the Finance Director/Chief Finance Officer (CFO) to review and respond in writing to all management letters or other internal control and compliance report findings and recommendations made by the independent auditor.

Audited financial statements, including the auditor's opinion thereon, will be submitted and presented to the Board of Directors by the independent accounting firm upon completion of the audit, after the financial statements have been reviewed and approved by the

Finance Director/Chief Finance Officer (CFO). The Board will review and accept the audited financial statement to conclude the audit.

Human Resources Policies and Procedures

The Employment

Nature of Employment

As an employee of the Olympic Council of Asia (OCA), it is important to understand the nature of your employment with the organization. OCA is committed to creating a positive and supportive work environment that fosters professional growth and development for all employees.

Employment Status:

All employees of OCA are considered to be full-time employees and are eligible for the benefits offered by the organization. All employment contracts are governed by the labor laws of the country in which the employee is based.

Job Descriptions:

All employees will be provided with a job description outlining their specific roles and responsibilities. These job descriptions are intended to provide clarity on the expectations for each role and to ensure that all employees are aware of their duties.

Probationary Period:

All new employees will be subject to a probationary period of six months, during which time their performance and suitability for the role will be assessed. This period may be extended for an additional three months if necessary.

Salary and Benefits:

Employees will receive a competitive salary and benefits package that is commensurate with their skills, experience, and responsibilities. Benefits include medical insurance, annual leave, sick leave, and other benefits as determined by the organization.

Working Hours:

Employees are expected to work a standard 48-hour week, from Sunday to Thursday, with Friday and Saturday being the weekend days. In certain situations, employees may be required to work additional hours or to work on weekends or public holidays, as determined by their manager.

Confidentiality:

All employees are expected to maintain the confidentiality of all confidential information related to the organization and its operations. This includes, but is not limited to, financial information, employee information, and any other information that is not intended for public dissemination.

Termination of Employment:

Employment with OCA may be terminated for any of the following reasons: resignation, retirement, termination for cause, or termination without cause. Termination of employment will be in accordance with the labor laws of the country in which the employee is based.

At OCA, we value our employees and are committed to providing a supportive and positive work environment. As an employee of the organization, it is important to understand the nature of your employment and the expectations for your role. By working together and upholding these standards, we can achieve our goals and ensure the success of the organization.

Employee Relations

OCA believes that the work conditions, wages, and benefits it offers to its employees are competitive with those offered by other employers in this area and in this industry. If employees have concerns about work conditions or compensation, they are strongly encouraged to voice these concerns openly and directly to their supervisors.

Our experience has shown that when employees deal openly and directly with supervisors, the work environment can be excellent, communications can be clear, and attitudes can be positive. We believe that OCA amply demonstrates its commitment to employees by responding effectively to employee concerns.

To protect and maintain direct employer/employee communications, we will do anything we can to protect the right of employees to speak for themselves.

Equal Employment Opportunity

To provide equal employment and advancement opportunities to all individuals, employment decisions at OCA will be based on merit, qualifications, and abilities. OCA does not discriminate in employment opportunities or practices based on race, color, religion, sex, national origin, age, or any other characteristic protected by law.

This policy governs all aspects of employment, including selection, job assignment, compensation, discipline, termination, and access to benefits and training.

Any employees with questions or concerns about any type of discrimination in the workplace are encouraged to bring these issues to the attention of their immediate supervisor or the Human Resource Department. Employees can raise concerns and make reports without fear of reprisal. Anyone found to be engaging in any type of unlawful discrimination will be subject to disciplinary action, up to and including termination of employment.

Diversity

We are opposed to all forms of unlawful and unfair discrimination. All employees, no matter whether they are part-time, full-time or temporary, will be treated fairly and with respect. When OCA selects candidates for employment, promotion, training or any other benefit, it will be on the basis of their aptitude and ability.

We recognize that our employees come from different backgrounds, cultures, and experiences, and we value the unique perspectives and ideas that they bring to our organization. By embracing diversity, we can create a more vibrant and dynamic workplace that fosters innovation and creativity.

To promote diversity and inclusion in our workforce, we actively seek out candidates from a wide range of backgrounds and experiences. We encourage all employees to share their ideas and perspectives, and we provide training and development opportunities to help our employees grow and succeed.

OCA is committed to:

- Create an environment in which the individual differences and contributions of all team members are recognized and valued;
- Create a working environment that promotes dignity and respect for every employee;
- Attract and retain a skilled and diverse workforce that best represents the talent available in the communities in which our assets are located and our employees reside;
- Ensure appropriate selection criteria based on diverse skills, experience and perspectives is used when hiring new staff. Job specifications, advertisements, application forms and contracts will not contain any direct or inferred discrimination;
- Ensure that applicants and employees of all backgrounds are encouraged to apply for and have fair opportunity to be considered for all available roles;
- Provide, to the greatest extent possible, universal access to safe, inclusive and accessible premises that allow everyone to participate and work to their full potential;
- Comply with equal opportunity and anti-discrimination legislation;
- Not tolerate any form of intimidation, bullying, victimization, vilification or harassment and to take disciplinary action against those who violate this policy;
- Provide training, development and advancement opportunities for all staff based on merit;
- Encourage anyone who feels they have been discriminated, to express their concerns so that we can take corrective action;
- Encourage employees to treat everyone with dignity and respect;
- Regularly review all our employment practices and procedures so that fairness is maintained at all times;
- Ensure to the greatest extent possible that all departments in OCA include representation of each gender;
- Set measurable objectives for gender diversity which will be monitored and reviewed against the effectiveness of this policy and associated procedures;

- Monitor and report annually on diversity and inclusion performance commitments.

Business Ethics and Conduct

At OCA, we are committed to conducting our business with the highest standards of ethics and integrity. Our employees are expected to adhere to these standards and ensure that their behavior aligns with our values and principles.

Code of Conduct

To guide our employees' behavior, we have established a Code of Conduct that outlines our expectations for ethical behavior. This code covers a range of topics, including conflicts of interest, bribery, corruption, discrimination, harassment, and confidentiality. All employees are required to read and sign the code of conduct upon joining the organization and are expected to abide by its principles throughout their employment.

Compliance with Laws and Regulations

We expect all employees to comply with all applicable laws and regulations, both local and international, that govern our business operations. This includes, but is not limited to, anti-bribery and anti-corruption laws, competition laws, and data protection laws. Employees who violate these laws or regulations may be subject to disciplinary action, up to and including termination of employment.

Confidentiality and Data Protection

At OCA, we handle a significant amount of confidential and sensitive information, including personal data of our employees, athletes, and partners. We expect our employees to maintain strict confidentiality regarding this information and to follow our data protection policies and procedures. Any breach of confidentiality or data protection may result in disciplinary action.

Whistleblower Policy

OCA has a whistleblower policy in place to encourage employees to report any concerns or suspected wrongdoing without fear of retaliation. Employees can report concerns to their immediate supervisor or to the designated compliance officer. All reports will be handled confidentially, and employees will not face any adverse action for making a report in good faith.

Responsibility to Partners and Sponsors

At OCA, we value our partnerships and sponsorships with various organizations and companies. We expect our employees to conduct themselves professionally and with integrity when dealing with our partners and sponsors. We do not tolerate any behavior that could damage the reputation or business interests of our partners or sponsors.

At OCA, we strive to conduct our business with the highest standards of ethics and integrity. We expect all our employees to adhere to our Code of Conduct and act in accordance with our values and principles. Failure to comply with these standards may result in disciplinary action, up to and including termination of employment. By upholding these ethical standards, we can maintain our reputation and integrity as a leading sports organization in Asia.

Personal Relationships in the Workplace

At the Olympic Council of Asia, we believe that creating a positive and respectful workplace culture is essential to the success of our organization. One aspect of this is maintaining appropriate personal relationships in the workplace.

We recognize that personal relationships may develop between employees, but it is important to keep these relationships professional and respectful to maintain a positive work environment. Unprofessional or inappropriate behavior can negatively impact the morale and productivity of the entire team, as well as lead to potential legal issues.

It is important to understand that favoritism or preferential treatment towards an employee involved in a personal relationship with another employee is not acceptable. This type of

behavior can create resentment and feelings of unfair treatment among other employees, which can ultimately harm the overall productivity and success of the organization.

In addition, it is important to recognize that romantic relationships may result in conflicts of interest, especially in situations where one employee has direct or indirect control over the other's work assignments or performance evaluations. This could lead to a perception of bias, even if the employee in question is acting in good faith.

To maintain a professional workplace environment, we require employees to disclose any personal relationships with other employees to their supervisor or HR representative. The purpose of this disclosure is to prevent conflicts of interest and ensure that all employees are treated fairly and objectively.

We encourage all employees to prioritize their work duties and responsibilities over personal relationships while at work. This means avoiding displays of affection, excessive personal conversations, and other behavior that could be perceived as unprofessional or disruptive to the work environment.

At the Olympic Council of Asia, we value diversity, respect, and professionalism in the workplace. By adhering to these principles, we can create a positive and productive work environment for all employees.

Conflicts of Interest

At OCA, we strive to maintain the highest level of integrity and ethical behavior in all aspects of our operations. We recognize that conflicts of interest may arise from time to time, and we are committed to managing these situations in a fair and transparent manner.

A conflict of interest occurs when an individual's personal interest interferes with their ability to make objective and impartial decisions in the best interest of OCA. Conflicts of interest can arise in various forms, including financial, personal, and professional relationships. Examples of conflicts of interest may include:

- An employee having a financial interest in a company that competes with OCA

- An employee using their position at OCA to benefit themselves or their family members
- An employee engaging in a personal relationship with a vendor or supplier of OCA

We take conflicts of interest very seriously and require all employees to disclose any potential conflicts of interest that may arise in their personal or professional life. Employees must disclose any relationship or financial interest that may interfere with their ability to make impartial decisions in the best interest of OCA.

In situations where a conflict of interest arises, we will take appropriate measures to manage the situation fairly and transparently. These measures may include:

- Disclosing the conflict of interest to affected parties and taking steps to manage any potential negative impact
- Removing the employee from any decision-making process related to the conflict of interest
- Terminating the employment of an employee who fails to disclose a conflict of interest

We also prohibit any form of retaliation against an employee who discloses a conflict of interest or raises concerns about potential conflicts of interest.

At OCA, we are committed to upholding the highest standards of integrity and ethical behavior in all our business practices. We believe that managing conflicts of interest transparently and fairly is essential to maintaining the trust and confidence of our stakeholders.

Should you be in doubt as to whether an activity involves a conflict, you should discuss the situation with your manager.

Outside Employment

OCA recognizes that employees may wish to engage in outside employment or activities in addition to their employment with the organization. However, outside employment and activities may pose conflicts of interest and may interfere with an employee's job performance, which can affect the organization's interests. As a result, OCA expects its employees to consider carefully the impact of outside employment or activities on their work performance and the potential conflicts of interest that may arise.

Prior Approval

Employees must obtain prior written approval from their supervisor and Human Resources department before engaging in any outside employment or activity. Failure to obtain prior approval may result in disciplinary action, up to and including termination.

Conflicts of Interest

Employees must avoid any outside employment or activity that could create a conflict of interest with OCA's interests. A conflict of interest exists when an employee's outside employment or activity interferes, or appears to interfere, with the employee's ability to perform his or her job duties, or when it creates a financial or personal gain that could influence the employee's judgment in the performance of their OCA duties.

If an employee is unsure whether an outside employment or activity creates a conflict of interest, they should disclose the situation to their supervisor and the Human Resources department for review.

Prohibited Activities

Employees may not engage in any outside employment or activity that:

- Competes with OCA's business activities or services
- Violates OCA's policies, procedures, or values
- Violates any applicable laws or regulations

Reporting Requirements

Employees must report any changes in their outside employment or activity to their supervisor and the Human Resources department immediately, including any changes in hours or job duties. Failure to report changes may result in disciplinary action, up to and including termination.

Disclaimer

OCA assumes no liability for any outside employment or activity undertaken by its employees. Employees engage in such activities at their own risk and expense and must ensure that such activities do not interfere with their job performance or create conflicts of interest.

Non-Disclosure

At OCA, we value the confidentiality of our business operations, including proprietary information, trade secrets, and other sensitive information. In order to protect these assets, we require all employees to sign a Non-Disclosure Agreement (NDA) as a condition of their employment.

The NDA is a legal document that outlines the terms and conditions of maintaining confidentiality and not disclosing any confidential information to third parties. By signing this agreement, employees agree to keep confidential information confidential, both during their employment with OCA and after their employment ends.

Examples of confidential information that employees are expected to keep confidential include but are not limited to:

* Compensation data
* Computer processes
* Computer programs and codes
* Partner and/or Supplier information
* Marketing and advertising plans
* Labor relations strategies
* Marketing strategies
* New materials research
* Pending projects and proposals
* Proprietary information
* Business plans and strategies
* Technical information
* Financial information
* Technological data
* Technological prototypes

Employees are also expected to take reasonable precautions to protect confidential information, including but not limited to:

- Not discussing confidential information in public areas
- Not using company-owned electronic devices to transmit confidential information outside of the company's network or approved channels
- Properly disposing of confidential information when it is no longer needed
- Protecting confidential information from theft, loss, or damage

Any employee who violates the terms of the NDA may face disciplinary action, up to and including termination of employment. Additionally, any violation of the NDA may result in legal action being taken against the employee.

At OCA, we take the protection of our confidential information seriously, and we expect all employees to uphold their commitment to maintain confidentiality and protect our valuable assets.

Disability Accommodation

OCA is ensuring equal opportunity in employment for qualified persons with disabilities. All employment practices and activities are conducted on a non-discriminatory basis.

Hiring procedures have been reviewed and provide persons with disabilities meaningful employment opportunities. Upon request, job applications are available in alternative, accessible formats, as is assistance in completing the application. Pre-employment inquiries are made only regarding an applicant's ability to perform the duties of the position.

Reasonable accommodation is available to all disabled employees, where their disability affects the performance of job functions. All employment decisions are based on the merits of the situation in accordance with defined criteria, not the disability of the individual.

Qualified individuals with disabilities are entitled to equal pay and other forms of compensation (or changes in compensation) as well as in job assignments, classifications, organizational structures, position descriptions, lines of progression and seniority lists. Leave of all types will be available to all employees on an equal basis.

OCA is also committed to not discriminating against any qualified employees or applicants because they are related to or associated with a person with a disability. OCA will follow any provincial or local law that provides individuals with disabilities greater protection.

This policy is neither exhaustive nor exclusive. OCA is committed to taking all other actions necessary to ensure equal employment opportunity for persons with disabilities in accordance with all applicable federal, provincial, and local laws.

Job Posting and Employee Referrals

OCA provides employees an opportunity to indicate their interest in open positions and advance within the organization according to their skills and experience. In general, notices of all regular, full-time job openings are posted, although OCA reserves its discretionary right to not post a particular opening.

Job openings will be posted on the employee bulletin board and/or in the email system, and normally remain open for 15 days. Each job posting notice will include the dates of the posting period, job title, department, location, grade level, job summary, essential duties, and qualifications (required skills and abilities).

To be eligible to apply for a posted job, employees must have performed competently for at least 90 calendar days in their current position. Employees who have a written warning on file or are on probation or suspension are not eligible to apply for posted jobs. Eligible employees can only apply for those posted jobs for which they possess the required skills, competencies, and qualifications.

To apply for an open position, employees should submit a job posting application to the Human Resource Department listing job-related skills and accomplishments. It should also describe how their current experience with OCA and prior work experience and/or education qualifies them for the position.

OCA recognizes the benefit of developmental experiences and encourages employees to talk with their supervisors about their career plans. Supervisors are encouraged to support employees' efforts to gain experience and advance within the organization.

An applicant's supervisor may be contacted to verify performance, skills, and attendance. Any staffing limitations or other circumstances that might affect a prospective transfer may

also be discussed. Job posting is a way to inform employees of openings and to identify qualified and interested applicants who might not otherwise be known to the hiring manager. Other recruiting sources may also be used to fill open positions in the best interest of the organization.

OCA also encourages employees to identify friends or acquaintances that are interested in employment opportunities and refer qualified outside applicants for posted jobs. Employees should obtain permission from the individual before making a referral, share their knowledge of the organization, and not make commitments or oral promises of employment.

An employee should submit the referral's resume and/or completed application form to the Human Resource Department for a posted job. If the referral is interviewed, the referring employee will be notified of the initial interview and the final selection decision.

Whistleblower Policy

OCA is committed to conducting its business with honesty and integrity at all times. If, at any time, this commitment is not respected or appears to be in question, OCA will endeavor to identify and remedy such situations. Therefore, it is the organization's policy to ensure that when a person has reasonable grounds to believe that an employee, manager or any other person related to the organization has committed, or is about to commit, an offence that could harm the organization's business or reputation, it denounces the wrongdoers in question.

The whistleblowing policy has been put in place to:

- Encourage employees, partners or managers to disclose this information or behavior; Protecting complainants from reprisals;
- Treated all parties to an investigation in a fair and equitable manner;
- To ensure confidentiality as much as possible;
- Take corrective and disciplinary action if wrongdoing is discovered.

- Providing false or misleading information, or withholding material information on OCA financial statements, accounting, auditing or other financial reporting fraud or misrepresentation;
- Pursuit of material benefit or advantage in violation of OCA's Conflict of Interest Policy; Misappropriation or misuse of OCA resources such as funds, supplies or other assets;
- Unauthorized alteration or manipulation of computer files;
- Destroying, altering, mutilating, concealing, covering up, falsifying, or making a false entry in any records that may be connected to an official proceeding, in violation of federal, provincial or state law or regulations or otherwise obstructing, influencing, or impeding any official proceeding, in violation of federal, provincial or state law or regulations;
- Violations of federal, provincial or state laws that could result in fines or civil damages payable by OCA, or that could otherwise significantly harm OCA's reputation or public image;
- Unethical business conduct in violation of any OCA policies and/or OCA Code of Conduct;
- Danger to the health, safety, or well-being of employees and/or the general public;
- Forgery or alteration of documents;
- Authorizing or receiving compensation for services not performed, or paying for services or goods that are not rendered or delivered;
- Authorizing or receiving compensation for hours not worked;
- Embezzling, self-dealing, or otherwise obtaining an unlawful private benefit (i.e., OCA assets being used by anyone in the organization improperly for personal gain).

It is the duty of all employees, contractual third parties or partners to report misconduct or suspected misconduct, including fraud and financial impropriety to the board. This includes misconducts such as but not limited to:

Accident and First Aid

OCA believes that the best practice in case of an accident, is to ensure staff have access to a trained First Aider or someone who can take charge in the event of an accident.

Details of these trained staff will be displayed from your line manager and you should familiarize yourself with names and contact details.

An Accident Book is also available from your line manager and it is the responsibility of everyone to report and record any accident involving personal injury.

Employees who are absent from work following an accident must complete a self-certification form, which clearly states the nature and cause of the injury.

Employment Status and Records

Employment Categories

It is the intent of OCA to clarify the definitions of employment classifications so that employees understand their employment status and benefit eligibility.

Each employee will belong to one other employment category:

Regular full-time employees are those who are not in a temporary or probation status and who are regularly scheduled to work OCA full-time schedule. Generally, they are eligible for OCA benefit package, subject to the terms, conditions, and limitations of each benefit program.

Regular part-time employees are those who are not assigned to a temporary or probation status and who are regularly scheduled to work less than 28 hours per week. While they do receive all legally mandated benefits, they are ineligible for all of OCA other benefit programs.

PROBATION is those whose performance is being evaluated to determine whether further employment in a specific position or with OCA is appropriate. Employees who

satisfactorily complete the probation period will be notified of their new employment classification.

CONTRACTUAL employees are those who are hired as interim replacements, to temporarily supplement the work force, or to assist in the completion of a specific project.

Access to Personnel Files

OCA maintains a personnel file on each employee. The personnel file includes such information as the employee's job application, resume, records of training, documentation of performance appraisals and salary increases, and other employment records.

Personnel files are the property of OCA, and access to the information they contain is restricted. Generally, only supervisors and management personnel of OCA who have a legitimate reason to review information in a file are allowed to do so.

Employees who wish to review their own file should contact the Human Resource Department. With reasonable advance notice, employees may review their own personnel files in OCA offices and in the presence of an individual appointed by OCA to maintain the files.

Personnel Data Changes

It is the responsibility of each employee to promptly notify OCA of any changes in personnel data. Personal mailing addresses, telephone numbers, number and names of dependents, individuals to be contacted in the event of emergency, educational accomplishments, and other such status reports should be accurate and current at all times. If any personnel data has changed, notify the Human Resource Department.

Probation Period

The probation period is intended to give new employees the opportunity to demonstrate their ability to achieve a satisfactory level of performance and to determine whether the new position meets their expectations. OCA uses this period to evaluate employee capabilities, work habits, and overall performance.

All new and rehired employees work on a probation basis for the first 90 calendar days after their date of hire. Any significant absence will automatically extend the probation period by the length of the absence. If OCA determines that the designated probation period does not allow sufficient time to thoroughly evaluate the employee's performance, the probation period may be extended for a specified period.

During the probation period, both parties may assess suitability for employment with the Employer. This also provides management an opportunity to assess skill levels and address areas of potential concern. During the first 90 days of the probationary period, employment may be terminated by either party for any reason whatsoever, with or without cause, and without notice or payment in lieu of notice.

Please take note that your manager’s role is to support you in developing and transferring your knowledge, skills and abilities to be successful in your job. We suggest you to take advantage of this resource.

Upon satisfactory completion of the probation period, employees enter the "Regular" employment classification.

During the probation period, new employees are eligible for those benefits that are required by law. After becoming regular employees, they may also be eligible for other OCA provided benefits, subject to the terms and conditions of each benefits program. Employees should read the information for each specific benefits program for the details on eligibility requirements.

Employment Applications

OCA relies upon the accuracy of information contained in the employment application, as well as the accuracy of other data presented throughout the hiring process and employment. Any misrepresentations, falsifications, or material omissions in any of this information or data may result in the exclusion of the individual from further consideration for employment or, if the person has been hired, termination of employment.

Performance Evaluation

At OCA, we believe that conducting regular performance evaluations is crucial to maintaining a high standard of performance, improving employee development, and achieving our organizational goals. Therefore, all employees will receive regular performance evaluations to assess their job performance, set goals, and provide feedback.

The performance evaluation process will occur annually, and the evaluation will be based on the employee's performance throughout the year. During the evaluation process, the employer and employee will review the objectives and the results achieved. Throughout the year, the employee and employer may refer to this document to track progress made toward objectives, highlight areas of concern, and indicate challenges identified along the way.

The performance evaluation will assess the employee's performance in several areas, including job knowledge and skills, quality of work, productivity, communication skills, teamwork, and adherence to organizational policies and procedures. The evaluation will also include a review of the employee's strengths and areas for improvement and provide constructive feedback.

The annual salary review of all employees is based on performance and is evaluated beginning in the month of January and effective on February 1st of each year. This evaluation will take into consideration the employee's overall performance during the previous year and their contributions to the organization.

The performance evaluation process is a collaborative effort between the employer and the employee, and open communication is encouraged throughout the process. Employees are also encouraged to provide feedback on their own performance and identify areas for growth and development.

The performance evaluation process is an essential tool in promoting employee development, providing constructive feedback, and fostering a culture of continuous improvement at OCA. By working together to set goals, assess performance, and provide

feedback, we can achieve our organizational goals and promote a positive work environment.

Job Descriptions

OCA makes every effort to create and maintain accurate job descriptions for all positions within the organization. Each description includes a job information section, a job summary section (giving a general overview of the job's purpose), an essential duties and responsibilities section, a qualifications section (including education and/or experience, language skills, mathematical skills, reasoning ability, and any certification required), and a KPI’s.

OCA maintains job descriptions to aid in orienting new employees to their jobs, identifying the requirements of each position, establishing hiring criteria, setting standards for employee performance evaluations, and establishing a basis for making reasonable accommodations for individuals with disabilities.

The hiring manager prepare job descriptions when new positions are created. Existing job descriptions are also reviewed and revised to ensure that they are up to date. Job descriptions may also be rewritten periodically to reflect any changes in the position's duties and responsibilities. All employees will be expected to help ensure that their job descriptions are accurate and current, reflecting the work being done.

Employees should remember that job descriptions do not necessarily cover every task or duty that might be assigned, and that additional responsibilities may be assigned as necessary. Contact the Human Resource Department if you have any questions or concerns about your job description.

Salary Administration

OCA is committed to providing competitive salaries that reflect employees' skills, experience, and job responsibilities. The organization's salary administration program is designed to ensure that salaries are fair, equitable, and consistent across all positions and departments.

Salary Structure:

OCA has established a salary structure that provides guidelines for determining salaries based on job responsibilities, skills, experience, and other factors. The salary structure includes a minimum and maximum salary range for each position, allowing for flexibility in compensation based on an employee's performance.

Salary Review:

OCA conducts an annual salary review for all employees, which is based on performance and evaluated on the anniversary of the employee's hire date. The evaluation process includes a review of the employee's job responsibilities, performance objectives, and accomplishments over the previous year. The salary review process also takes into account market conditions and industry standards to ensure that salaries remain competitive.

Merit Increases:

Merit increases are awarded based on the employee's performance over the previous year and are determined based on the salary structure for the employee's position. Merit increases may be awarded to employees who have exceeded performance expectations, made significant contributions to the organization, or taken on additional responsibilities.

Promotions and Transfers:

When an employee is promoted or transferred to a new position within the organization, the employee's salary will be reviewed based on the new job responsibilities and salary structure for the new position. OCA is committed to ensuring that employees are fairly compensated for their skills and experience and that salary increases are consistent with industry standards.

Salary Adjustments:

OCA may adjust salaries outside of the annual review process in certain circumstances, such as to correct a salary that is not competitive with industry standards or to address significant changes in job responsibilities.

Incentive bonuses:

Employee bonuses are awarded based on a variety of factors, including individual performance, team performance, and organizational performance. The specific criteria and amount of the bonus may vary depending on the employee's job level and the nature of their work.

The process for awarding bonuses typically begins with the establishment of performance goals and objectives at the beginning of the year. Throughout the year, employees are evaluated based on their progress towards these goals, as well as their overall job performance and contribution to the organization.

At the end of the year, employee performance is reviewed, and bonuses are awarded based on the extent to which these performance goals were met or exceeded. The amount of the bonus may also be influenced by a variety of factors.

It is important to note that bonuses are typically not guaranteed, and their availability and amount may be subject to change depending on the financial health and priorities of the organization. Additionally, bonus awards may be pro-rated based on the employee's start date or the duration of their employment during the evaluation period.

Confidentiality:

Salary information is confidential and will only be disclosed on a need-to-know basis. Employees are expected to maintain the confidentiality of their salary information and not discuss it with other employees.

At OCA, we are committed to providing competitive salaries that reflect employees' skills, experience, and job responsibilities. Our salary administration program ensures that salaries are fair, equitable, and consistent across all positions and departments.

Professional Development

At the discretion of your manager/supervisor, employees may be able to attend conferences, courses, seminars and meetings, identified through annual work plans and performance reviews, which may be beneficial to the employee’s professional

development. When these opportunities are directly related to the employee's position, or are suggested by the manager/supervisor, then OCA will cover the cost of registration, course materials and some travel expenses.

If OCA has agreed to pay for a course, the fees will be paid on evidence of successful completion. If the OCA sponsors a course (or courses) and the employee departs the OCA within a year of completion, the course fees will become repayable in full.

Employee Benefit Programs

Employee Benefits

At OCA, we value the hard work and dedication of our employees, and we are committed to providing them with a comprehensive employee benefits package to support their health, well-being, and financial security. Our employee benefit programs are designed to meet the diverse needs of our workforce, and we strive to provide competitive benefits that align with industry standards and best practices.

We offer a comprehensive health insurance plan that includes medical, dental, and vision coverage. We also provide access to health and wellness resources, such as fitness discounts.

Vacation Benefits

Annual Leave:

All employees are entitled to thirty (30) working days of paid leave per year, exclusive of public holidays and Fridays. Employees who have completed one year of continuous service with OCA are eligible for annual leave. Annual leave must be taken within the year it is earned, and it can be carried over for a maximum of 2 years leave balance (60 days). Employees are encouraged to plan their annual leave in advance and obtain approval from their immediate supervisor.

Air Ticket:

OCA will provide one economy class air ticket for the employee to travel from Kuwait to their country of residence, as well as 50% of the economy class airfare for the employee's spouse and up to two children.

Public Holidays and Fridays:

In addition to annual leave, employees are entitled to all public holidays and Fridays, as declared by the government of Kuwait. If an employee is required to work on a public holiday or Friday, they will be compensated according to the Kuwait Labor Law.

Application Procedure:

Employees who wish to take annual leave must apply for it at least two (2) weeks in advance. The employee's immediate supervisor must approve the application. If two (2) or more employees apply for annual leave at the same time, preference will be given to the employee who applied first. However, the final decision will be at the discretion of the management.

Haj and Umrah Leave

Hajj and Umrah are important religious pilgrimages for Muslims, and OCA recognizes the significance of these events. OCA provides eligible employees with Hajj and Umrah leave to perform these religious duties.

Eligible employees who have completed one year of continuous service with OCA are entitled to take up to 1 week of Umrah leave and 1 month of Hajj leave, which is paid time off. This leave can be taken once in a lifetime, and it must be taken within the employee's first five years of eligibility.

To be eligible for Hajj and Umrah leave, employees must provide documentation of their pilgrimage from the relevant authority or institution, and this documentation should be submitted to the HR department at least one month prior to the intended leave start date. The HR department will review and approve the leave request based on the company's policy and the employee's eligibility.

During Hajj and Umrah leave, employees will continue to receive their regular salary, and they will also be entitled to the benefits that they would have received had they been working during that time. However, any expenses related to the pilgrimage, such as airfare and accommodation, will be the employee's responsibility.

Holidays

OCA will grant holiday time off to all employees on the holidays listed below:

- New Year's Day
- Isra and Miraj
- National Day
- Liberation Day

- Eid al-Fitr
- Waqfat Arafat Day
- Eid al-Adha
- Islamic New Year
- The Prophet's Birthday

Employees are entitled to the holidays listed above. If an employee is required to work on a holiday, they will be compensated according to Kuwait labor laws. Employees who are required to work on a holiday will receive a day off in lieu or will be paid at an overtime rate.

OCA encourages all employees to take time off during holidays to spend with their family and friends. Please note that any employee who fails to show up to work on a scheduled workday immediately before or after a holiday may be subject to disciplinary action.

Workers Insurance

OCA provides Basic Employment Insurance program at no cost to employees. This program covers any injury or illness sustained in the course of employment that requires medical, surgical, or hospital treatment.

Employees who sustain work-related injuries or illnesses should inform their supervisor immediately. No matter how minor an on-the-job injury may appear, it is important that it be reported immediately. This will enable an eligible employee to qualify for coverage as quickly as possible. Neither OCA nor the insurance carrier will be liable for the payment of workers' compensation benefits for injuries that occur during an employee's voluntary participation in any off-duty recreational, social, or athletic activity sponsored by OCA.

Sick Leave Benefits

OCA recognizes that employees may require time off due to illness or injury. To support our employees during such times, we offer sick leave benefits to eligible employees.

Eligibility:

All regular full-time employees are eligible for sick leave benefits.

Sick Leave Entitlement:

Employees are entitled to 15 days of sick leave per year at full pay. To qualify for sick leave, employees must provide a medical report endorsed by the government medical authority. In the event of any conflict regarding the necessity of sick leave or its duration, the report of the government doctor will be adopted.

Exceeding Sick Leave Entitlement:

If sick leave exceeds 15 days per year, 25% of the monthly salary will be deducted.
If a sick leave exceeds 25 days per year, 50% of the monthly salary will be deducted.
If a sick leave exceeds 35 days per year, 75% of the monthly salary will be deducted.
If a sick leave exceeds 45 days per year, no salary will be paid.

Work-Related Illness or Injury:

If an employee is exposed to injury or illness during their official work or assignment by their supervisor or manager, the supervisor or manager may exclude the deduction stipulated above.

Notification:

Employees must inform their immediate supervisor or HR department as soon as possible in the event of illness or injury that requires absence from work. Failure to report the illness or injury may result in disciplinary action.

Return to Work:

Employees must provide a medical clearance certificate before returning to work after a sick leave. In the event of a chronic illness, the medical clearance certificate should specify the employee's fitness to work and any restrictions on their duties.

OCA reserves the right to request additional medical reports or examinations to verify the medical condition of the employee.

We believe that a healthy workforce is essential to our success as an organization, and we strive to provide our employees with the necessary support during times of illness or injury.

Bereavement Leave

Employees who require taking time off due to the death of an immediate family member should notify their supervisor immediately.

OCA provides paid bereavement leave for employees who have worked for at least 60 calendar days. In the case of the death of an employee's father, mother, sister, brother, spouse, child, or the employee's spouse's child, the employee will be granted three (3) working days of paid bereavement leave. This leave is intended to allow the employee time to grieve and attend to any necessary arrangements related to the loss of their loved one.

Bereavement pay is calculated based on the base pay rate at the time of absence and will not include any special forms of compensation, such as incentives, commissions, bonuses, or shift differentials.

Health Insurance

Health insurance is an important benefit that OCA provides to its employees. It is essential for our employees to have access to quality healthcare and medical services for themselves and their families. OCA provides health insurance coverage to its employees and their eligible dependents, as per the terms and conditions outlined in this policy.

Eligibility:

All full-time employees of OCA and their eligible dependents are eligible for health insurance coverage. Eligible dependents include the employee's spouse and unmarried children up to the age of 18 or up to the age of 25 if they are studying full-time in an accredited educational institution.

Coverage:

The health insurance coverage provided by OCA includes:

- Inpatient and outpatient medical services
- Diagnostic and laboratory tests
- Prescription drugs
- Emergency care
- Specialist consultations

- Maternity services
- Dental services

Premiums:

OCA pays the full cost of the employee's health insurance coverage. If an employee wishes to add eligible dependents to their coverage, they will be required to pay a portion of the monthly premiums, as per the prevailing rates.

Claims Process:

Employees are required to follow the claims process as outlined by the health insurance provider. This includes obtaining prior authorization for medical procedures, submitting claims within the required time frame, and providing all necessary documentation.

Renewal:

Health insurance coverage is renewed annually. The employee will be notified of any changes to the coverage or premiums prior to the renewal date.

Termination:

Health insurance coverage will be terminated upon termination of employment.

Life Insurance

Life insurance offers you and your family important financial protection. OCA provides a basic life insurance plan for eligible employees.

Accidental Death and Dismemberment (AD&D) insurance provides protection in cases of serious injury or death resulting from an accident. AD&D insurance coverage is provided as part of the basic life insurance plan. Employees in the following employment classifications are eligible to participate in the life insurance plan:

Regular full-time employees

Eligible employees may participate in the life insurance plan subject to all terms and conditions of the agreement between OCA and the insurance carrier. Contact the HR Department for more information about life insurance benefits.

Maternity Leave

Maternity Leave Admissibility

Maternity leave is a benefit that is provided to female employees who are expecting or have recently given birth to a child. At OCA, we recognize the importance of this time in a mother's life and we are committed to supporting our female employees during this period.

Female employees who have been working with OCA for a minimum of one year are eligible for maternity leave. The duration of the maternity leave will be for a period of 30 calendar days, with full pay. It may be possible for employees to take an additional period of 30 calendar days off due to child care.

Notice:

a) The employee must provide in writing to the organization, at least three weeks in advance the date of the beginning of her maternity leave and the date envisaged of her return to work. A medical certificate attesting of the date envisaged of the birth must accompany the notice.

b) The notice can be less than 3 weeks if the medical certificate attests need for the employee to cease working within a less time. If physical dangers are possible, the employee will be assigned to other tasks while preserving the rights and preferences connected to her regular position.

Complications:

If the employee or the child suffers from complications preventing the return to work at the end of the maternity leave, the employee will have to forward a medical certificate to the organization.

Return to work:

a) The employee must provide in writing to management the expected date of her return to work and this, three (3) weeks before returning from his maternity leave.

b) The employee who does not present himself to work five (5) days after the expiration of his maternity leave may be known to have resigned.

c) The direction can require of the employee who returns to work two (2) weeks after her childbirth, the production of a medical certificate attesting of its sufficient re-establishment to resume work.

Special maternity leave:
When there is a danger of miscarriage, or a danger to the health of the mother or of the child to come caused by pregnancy and requiring a stop of work, the employee is entitled to a special maternity leave of the duration prescribed by the medical certificate which attests existing danger and which indicates the date envisaged of the childbirth.

Timekeeping / Payroll

Timekeeping
All employees are required to record their daily work hours, including arrival and departure times, using the OCA's designated timekeeping system. Any adjustments or corrections to recorded time must be made promptly and submitted to the HR department for approval. Failure to accurately record time may result in delayed payment or disciplinary action.

Paydays
Payday for all employees is on the last working day of each month. In the event that the regular payday falls on a weekend or public holiday, the pay will be issued on the preceding workday. All employees will be paid through direct deposit to a bank account designated by the employee. It is the responsibility of each employee to ensure that their payroll information, including bank account and tax information, is up to date and accurate.

In the event of any payroll discrepancies or errors, employees must notify the HR department as soon as possible. OCA will investigate the issue and make necessary corrections promptly.

OCA has the right to stop salary payment in case the employee is absent from duty for 7 continuous or intermittent days or more than 20 days in a 12-month period. The HR department will inform the employee of the salary stoppage and the reason for it.

Employment Termination

The OCA believes in maintaining a positive and constructive work environment. However, circumstances may arise that result in the termination of an employee's employment. In such cases, the OCA will follow the below-mentioned guidelines:

Notice Period:

The OCA will provide a notice of 90 days paid leave (3 months) to the employee before the termination of the employment contract.

Payment Calculation:

- If the employee has worked continuously with OCA for less than 5 years, he/she will be entitled to receive 15 days of paid leave per each service year (based on last month's salary).
- If the employee has worked continuously with OCA for more than 5 years, he/she will be entitled to receive one month's salary per each worked year (based on last month's salary). However, the total payment should not exceed 18 months' salary.
- In addition to the above, the employee is entitled to encash a maximum of two years' unused leave.

It is important to note that any outstanding debts owed to the OCA will be deducted from the final settlement amount.

The OCA reserves the right to terminate an employee's employment without notice or payment in lieu of notice in the following circumstances:

- If the employee violates the terms and conditions of the employment contract.
- If the employee is found guilty of misconduct, insubordination, or any other behavior that is detrimental to the interests of the OCA.
- If the employee is found to be engaged in any illegal activity or unethical behavior that may harm the reputation of the OCA.

Upon termination of employment, the employee is required to return all company-owned property and equipment, including but not limited to laptops, phones, keys, access cards,

etc. The OCA will provide a service certificate and all other necessary documents to the employee on request.

Work Conditions and Hours

Attendance and Punctuality

The normal work schedule for all employees is 8 hours a day, Sunday to Thursday. Supervisors will advise employees of the times their schedules will normally begin and end. Staffing needs and operational demands may necessitate variations in starting and ending times, as well as variations in the total hours that may be scheduled each day and week.

Flexible scheduling, or flextime, is available in some cases to allow employees to vary their starting and ending times each day within established limits. Flextime may be possible if a mutually workable schedule can be negotiated with the supervisor involved. However, such issues as staffing needs, the employee's performance, and the nature of the job will be considered before approval of flextime. Employees should consult their supervisor to request participation in the flextime program.

Absences

As an employee, you will be treated as a professional, which means that you will be expected to complete your work on time and at the expected level of quality. If extra hours are needed to complete your work, you will be expected to put in those extra hours. If, on the other hand, you are able to complete your work in less than a standard workweek, you are free to use those extra hours as you see fit. In return for being treated as a professional, we expect you to behave as one and not to abuse these privileges.

Even though you will be treated as a professional and will presumably behave as one, general absence guidelines are nevertheless necessary to ensure that we are able to conduct business in a predictable manner. Although we are not interested in monitoring your comings and goings, we need to know, in advance where possible, when you will be absent from work. Here are those guidelines:

Absences

Employees are expected to be at work and to work a full workweek, except for authorized absences. Authorized absences include the following:

- Vacation time scheduled in advance
- Sick leave
- Time off for a workers' compensation injury
- A death in your family
- Emergency situations beyond your control

Notification procedure

To obtain an authorized absence, call in, where possible, and let the appropriate person know that you are unable to come to work. The call should be made, if possible, no later than your regular starting time.

Failure to notify

If you are unable to come to work, you must inform your supervisor in advance and provide an explanation for your absence. Failure to do so may result in disciplinary action, up to and including termination.

It is important to note that the employee cannot be absent from duty for more than 7 consecutive days or more than 20 days intermittently per year, unless there is a personal reason connected to the employee. In such cases, OCA reserves the right to terminate the employee contract automatically without prior notice.

Inclement weather

During inclement weather, you should call to find out whether to report to work. Also, while the weather may be nice where you are, hazardous weather conditions could exist at or near the workplace. If you know hazardous conditions have been reported in the area, protect yourself and call work first.

Use of Cell Phone

At OCA, employees are allowed to use cell phones at work, but it is important to ensure that they do not distract from the employee's work or disrupt the workplace. To this end, OCA requests that each employee follow a few simple rules.

Cell phones should be used in a manner that benefits the work, such as business calls, productivity apps, and calendars. Personal calls should be kept brief, and if possible, the employee should use an empty meeting room or common area so as not to disturb colleagues. Playing games on the phone or texting excessively should be avoided, as well as using the phone for any reason while driving a company vehicle. Employees should not use the phone to record confidential information, and they should not download or upload inappropriate, illegal, or obscene material using the corporate internet connection.

Violation of these policies can result in disciplinary action, including termination. Employees who fail to comply with these policies will be subject to corrective action, up to and including termination.

Smoking

OCA is committed to providing a healthy and safe work environment for all employees. Therefore, smoking is prohibited in all OCA premises, including indoor and outdoor areas. This policy applies to all employees, contractors, visitors, and customers.

Employees who wish to smoke during breaks or lunchtime must leave OCA premises and smoke outside of the designated smoking area. Smoking outside of the designated smoking area is strictly prohibited.

Smoking is defined as the use of any tobacco product, including but not limited to cigarettes, cigars, pipes, and smokeless tobacco products. The use of electronic cigarettes or vaping devices is also prohibited on OCA premises.

This policy applies equally to all employees, customers, and visitors.

Overtime

At OCA, overtime means working beyond the normal working hours at the HQ office. Overtime work is only allowed with prior approval from the employee's supervisor or

department head. Overtime work may be necessary due to the workload and urgency of the task.

The extra time worked must be recorded accurately by the OCA Finance department on a monthly basis. The Finance Department must obtain approval from the CFO for the recorded extra time at the end of each month. The Finance Director/Chief Finance Officer (CFO) must then seek approval from the OCA CEO/Director General before discharging payment for the overtime worked.

It is important to note that any extra working time during the Asian Games, General Assembly, and other meetings outside the OCA HQ will not count as an overtime period.

OCA employees are entitled to receive overtime pay for the extra time worked. The overtime rate will be determined based on the employee's base hourly rate. The overtime rate will be 1.5 times the base hourly rate for any extra time worked on weekdays, and 2 times the base hourly rate for any extra time worked on weekends and public holidays.

It is the responsibility of the employee to accurately record and report the extra time worked to their supervisor or department head. Failure to report the extra time worked accurately may result in delayed payment or no payment for the overtime worked.

OCA values the work-life balance of its employees and encourages them to avoid unnecessary overtime work. However, when overtime work is necessary, OCA expects its employees to comply with the rules and regulations regarding overtime work.

Use of Equipment

Equipment essential in accomplishing job duties is often expensive and may be difficult to replace. When using property, employees are expected to exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines.

Please notify the supervisor if any equipment, machines, or tools appear to be damaged, defective, or in need of repair. Prompt reporting of damages, defects, and the need for repairs could prevent deterioration of equipment and possible injury to employees or

others. The supervisor can answer any questions about an employee's responsibility for maintenance and care of equipment used on the job.

The improper, careless, negligent, destructive, or unsafe use or operation of equipment can result in disciplinary action, up to and including termination of employment.

Remote work or Work from Home (WFH)

Remote work or Work from Home (WFH) is an arrangement where employees can work outside of the traditional office setting, either partially or completely, by using technology to communicate and collaborate with colleagues and complete their job duties. This policy applies to all regular full-time and part-time employees of the Olympic Council of Asia (OCA).

Remote work may be allowed on a case-by-case basis, as determined by the employee's supervisor and approved by the OCA Chief Operating Officer (COO). Approval for remote work will depend on the nature of the work, the employee's job duties, and the employee's performance and productivity record.

Employees who work remotely must comply with all OCA policies and procedures, including those related to data security and confidentiality. Employees must use only authorized devices and applications to access OCA data, and must follow all security protocols to ensure the security and privacy of OCA information.

The following guidelines must be followed by employees who work remotely:

- Work Schedule: Employees must follow their regular work schedule and comply with all deadlines and deliverables. Employees must inform their supervisor of their availability and work schedule.
- Work Environment: Employees must ensure that their work environment is free from distractions, safe, and conducive to work. Employees must have a dedicated workspace, a reliable internet connection, and a functioning computer or laptop.
- Communication: Employees must be available to communicate during their regular work hours and respond to emails and phone calls in a timely manner.
- Productivity: Employees must maintain productivity levels while working remotely, and must report their work progress and accomplishments to their supervisor.

- Attendance: Employees must inform their supervisor if they are unable to work remotely due to illness, personal reasons, or technical difficulties.
- Equipment: Employees must use only authorized devices and software for remote work. Employees must report any technical difficulties to the IT department immediately.
- Expenses: Employees are responsible for any additional expenses incurred while working remotely, such as internet and phone charges, office supplies, or equipment.

Remote work may be terminated by the OCA at any time, with or without cause, and employees may be required to return to the office at any time, depending on the needs of the organization. The OCA acknowledges that remote work may provide benefits for employees and the organization. The OCA encourages supervisors to work with employees to determine if remote work is a viable option, based on the nature of their job duties and the needs of the organization.

Emergency Closing

The OCA recognizes that emergency situations such as inclement weather, natural disasters, or other unforeseeable events may occur that could impact the safety and well-being of its employees. In such cases, the OCA may need to close its offices or require employees to work remotely.

Notification of Emergency Closings:

In the event of an emergency closing, the OCA will make every effort to notify employees as soon as possible through the following communication channels:

- Email: An email will be sent to all employees notifying them of the closing and any additional information they need to know.
- OCA Website: The OCA website will be updated with a notice of the closing and any relevant information.
- Local Media: If appropriate, the OCA will notify local media outlets of the closing.

Employee Responsibilities:
In the event of an emergency closing, employees are responsible for the following:

- Checking for Updates: Employees must check their email, the OCA website, and local media for updates on the status of the emergency closing.
- Contacting Their Supervisor: Employees must contact their supervisor to determine their work schedule and any additional instructions.
- Safety: Employees must prioritize their safety and the safety of their families during emergency situations.
- Reporting Absences: Employees who are unable to work remotely or attend work during an emergency closing must notify their supervisor as soon as possible.

Compensation during Emergency Closings:
Employees will be compensated for their work during an emergency closing period in accordance with their regular compensation policies. If the emergency closing results in a disruption of work that affects an employee's ability to work and earn their regular pay, the OCA may offer alternative work assignments or pay them in accordance with its policies for missed work due to unforeseen circumstances.

The OCA will make every effort to ensure the safety and well-being of its employees during emergency situations while maintaining business continuity.

Business Travel Expenses
OCA will reimburse employees for reasonable business travel expenses incurred while on assignments away from the normal work location. All business travel must be approved in advance by the immediate supervisor.

Employees whose travel plans have been approved should make all travel arrangements through OCA travel department. When approved, the actual costs of travel, meals, lodging, and other expenses directly related to accomplishing business travel objectives will be reimbursed by OCA. Employees are expected to limit expenses to reasonable amounts.

Expenses that generally will be reimbursed include the following:

- Airfare or train fare for travel in coach or economy class;
- Car rental fees, only for compact or mid-sized cars;
- Fares for shuttle or airport bus service, where available; costs of public transportation for other ground travel;
- Taxi fares, only when there is no less expensive alternative;
- Mileage costs for use of personal cars, only when less expensive transportation is not available;
- Cost of standard accommodations in low to mid-priced hotels, motels, or similar lodgings;
- Cost of meals, no more lavish than would be eaten at the employee's own expense;
- Charges for telephone calls and similar services for business purposes;
- Charges for laundry only on trips of five or more days (Personal entertainment and personal care items are not reimbursed).

Employees are encouraged to use their cellular telephone or calling cards when traveling, as hotel charges are excessive.

Employees who are involved in an accident while traveling on business must promptly report the incident to their immediate supervisor. Vehicles owned, leased, or rented by OCA may not be used for personal use without prior approval.

Cash advances of $100.00/day to cover reasonable anticipated expenses may be made to employees, after travel has been approved. Employees should submit a written request to their supervisor when travel advances are needed.

When travel is completed, employees should submit completed travel expense reports within 30 days. Reports should be accompanied by receipts for all individual expenses.

Employees should contact their supervisor for guidance and assistance on procedures related to travel arrangements, travel advances, expense reports, reimbursement for specific expenses, or any other business travel issues.

Abuse of this business travel expenses policy, including falsifying expense reports to reflect costs not incurred by the employee, can be grounds for disciplinary action, up to and including termination of employment.

Visitors in the Workplace

The OCA welcomes visitors to its premises, but it is important that visitors are aware of our policies and procedures to ensure their safety and the safety of our employees. This policy outlines the procedures to be followed when visitors are in the workplace.

Identification and Sign-In:

All visitors to the OCA workplace must provide a valid identification card such as a driver's license or passport to the receptionist or security personnel. Visitors will be required to sign in and out of the building and provide a reason for their visit.

Escort Policy:

Visitors must be escorted by an OCA employee at all times while they are in the building. The employee who is escorting the visitor is responsible for ensuring that the visitor is aware of the location of emergency exits and the assembly point in the event of an emergency.

Safety and Security:

Visitors are required to comply with the OCA's health and safety policies and procedures while they are on the premises.

Confidentiality:

Visitors are reminded that they must not disclose any confidential or proprietary information of the OCA during their visit. Visitors who need to access such information must sign a non-disclosure agreement before being granted access to such information.

Visitors with Disabilities:

The OCA is committed to ensuring that visitors with disabilities have access to our premises. Visitors with disabilities must notify the OCA in advance of their visit so that we can make any necessary accommodations.

Photography and Recording:

Photography and recording of any kind are prohibited within the OCA workplace without the prior permission of the OCA. This includes the use of mobile phones and other electronic devices.

Gifts and Donations:

Visitors are not permitted to offer gifts or donations to OCA employees or request personal favors from OCA employees during their visit.

Termination of Visit:

The OCA reserves the right to terminate the visit of any visitor who breaches any of the policies and procedures outlined in this document or who poses a threat to the safety and security of the OCA and its employees.

The OCA expects all employees to comply with the procedures outlined in this policy. If you have any questions or concerns about this policy, please contact your supervisor or HR representative for further guidance.

Computer and Email Usage

Computer and email usage are essential components of OCA's daily operations. All employees are expected to use OCA's computer and email systems responsibly and professionally. The following guidelines should be followed at all times:

Proper Use of OCA's Computer Systems:

Employees should use OCA's computer systems for work-related purposes only. Personal use of OCA's computer systems is prohibited. Employees must follow these guidelines when using OCA's computer systems:

- Employees must not use OCA's computer systems to engage in any activity that violates local or international laws or regulations.
- Employees must not use OCA's computer systems to access or download any inappropriate, illegal, or offensive material, such as pornography or hate speech.
- Employees must not install or use unauthorized software on OCA's computer systems.
- Employees must not modify, damage, or destroy OCA's computer systems or any data stored on them.
- Employees must not attempt to gain unauthorized access to OCA's computer systems or any data stored on them.
- Employees must not disclose their login credentials to anyone else.
- Employees must log out of their computer systems before leaving their workstations.

Proper Use of Email:

Email is an important communication tool used by OCA to communicate with employees and external parties. The following guidelines should be followed when using OCA's email system:

- Employees should use OCA's email system for work-related purposes only. Personal use of OCA's email system is allowed, but it should not interfere with work-related tasks.
- Employees must not use OCA's email system to send inappropriate, illegal, or offensive material, such as pornography or hate speech.
- Employees must not send unsolicited emails or spam.
- Employees must not send emails that contain confidential information unless the recipient is authorized to receive such information.
- Employees must not forward emails that contain confidential information to unauthorized parties.
- Employees must not impersonate another employee or an external party in an email.
- Employees must not use email to engage in any activity that violates local or international laws or regulations.

Security and Confidentiality:

Employees have a responsibility to protect OCA's computer systems and data from unauthorized access and protect confidential information. The following guidelines should be followed to ensure security and confidentiality:

- Employees must use strong passwords and must not share them with anyone.
- Employees must not access, modify, or disclose confidential information unless authorized to do so.
- Employees must report any suspicious activity or security breaches to their supervisor or IT department immediately.
- Employees must lock their workstations when leaving their desk, and they must not leave confidential information on their screen.
- The employee should never use the corporate computer or email for any illegal activities, including piracy or hacking.
- Employees must not download, install or run any software, script, application or program without prior approval from the IT department. This includes freeware, shareware, or any other type of software that is not already installed on the company’s computers.
- Employees are prohibited from using the corporate computer or email for any activity that could damage the reputation of the company or its employees, such as posting defamatory comments on social media or sending inappropriate messages to customers or vendors.
- OCA reserves the right to monitor any activity on its computers, including email and internet usage, in order to ensure compliance with company policies and applicable laws.
- The employee should not use the company email to send or receive large attachments, such as video or music files, or to send emails to large groups of people unless it is work-related and necessary.
- The employee should not use the company email for personal or political purposes or to forward chain letters or other types of spam messages.
- The employee should be aware of phishing attempts, and should never give out sensitive information such as passwords or social security numbers in response to an email request, even if it appears to come from a legitimate source.

- Employees are responsible for maintaining the security of their passwords and must not share them with anyone, including colleagues and family members.
- Employees must report any security breaches or suspected security breaches to their supervisor or the IT department immediately.

OCA takes its computer and email usage policies seriously, and any violations of these policies may result in disciplinary action, up to and including termination. By using the company's computers and email systems, employees agree to comply with these policies and to use these resources only for work-related purposes.

Internet Usage

Internet access to global electronic information resources on the World Wide Web is provided by OCA to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage. While Internet usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of OCA and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of OCA. As such, OCA reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could

reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a rule, if an employee did not create the material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

Internet users should take the necessary anti-virus precautions before downloading or copying any file from the Internet. All downloaded files are to be checked for viruses; all compressed files are to be checked before and after decompression.

Abuse of the Internet access provided by OCA in violation of law or OCA policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy.

The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions;
- Sending or posting messages or material that could damage the organization's image or reputation;
- Participating in the viewing or exchange of pornography or obscene materials;
- Sending or posting messages that defame or slander other individuals;
- Attempting to break into the computer system of another organization or person;
- Refusing to cooperate with a security investigation;
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;
- Using the Internet for political causes or activities, religious activities, or any sort of gambling;
- Jeopardizing the security of the organization's electronic communications systems;
- Sending or posting messages that disparage another organization's products or services;
- Passing off personal views as representing those of the organization;
- Sending anonymous email messages;
- Engaging in any other illegal activities.

Workplace Monitoring

Workplace monitoring refers to the observation and surveillance of employees by the company to ensure that they are following workplace policies and procedures, and to protect the company's interests. Monitoring can take many forms, including physical observation, electronic surveillance, and software tracking.

OCA reserves the right to monitor and track employee activities in the workplace. This includes the use of company-owned devices and networks, as well as personal devices used for work-related purposes. Monitoring may be conducted through the use of CCTV cameras, email monitoring software, internet usage tracking, and other similar methods.

The purpose of workplace monitoring is to ensure that employees are complying with company policies and procedures, and to prevent or investigate any potential violations. OCA recognizes that employee privacy is important and will strive to balance the need for monitoring with employee privacy rights.

Employees should not have any expectation of privacy when using company-owned devices or networks, or when using personal devices for work-related purposes. Employees should also be aware that any communication or activity conducted on company-owned devices or networks, or using personal devices for work-related purposes, may be monitored and tracked.

To protect employee privacy, OCA will not monitor personal communications that are unrelated to work activities. However, OCA reserves the right to monitor and track any communication or activity that may impact the company's reputation, security, or operations.

Any monitoring or tracking conducted by OCA will be done in accordance with applicable laws and regulations, and will be communicated to employees in advance, to the extent practicable. Employees who have questions or concerns about workplace monitoring should contact their supervisor or the HR department for further information.

Workplace Violence Prevention

OCA is committed to preventing workplace violence and to maintaining a safe work environment. OCA has adopted the following guidelines to deal with intimidation, harassment, or other threats of (or actual) violence that may occur during business hours or on its premises.

All employees, including supervisors and temporary employees, should be treated with courtesy and respect at all times. Employees are expected to refrain from fighting, "horseplay," or other conduct that may be dangerous to others.

Conduct that threatens, intimidates, or coerces another employee, a customer, or a member of the public at any time, including off-duty periods, will not be tolerated. This prohibition includes all acts of harassment, including harassment that is based on an individual's sex, race, age, or any characteristic protected by federal, provincial, or local law.

All threats of (or actual) violence, both direct and indirect, should be reported as soon as possible to your immediate supervisor or any other member of management. This includes threats by employees, as well as threats by partners, vendors, or other members of the public. When reporting a threat of violence, you should be as specific and detailed as possible.

All suspicious individuals or activities should also be reported as soon as possible to a supervisor. Do not place yourself in peril. If you see or hear a commotion or disturbance near your workstation, do not try to intercede or see what is happening.

OCA will promptly and thoroughly investigate all reports of threats of (or actual) violence and of suspicious individuals or activities. The identity of the individual making a report will be protected as much as is practical. In order to maintain workplace safety and the integrity of its investigation, OCA may suspend employees, either with or without pay, pending investigation.

Anyone determined to be responsible for threats of (or actual) violence or other conduct that is in violation of these guidelines will be subject to prompt disciplinary action up to and including termination of employment.

OCA encourages employees to bring their disputes or differences with other employees to the attention of their supervisors or the Human Resource Department before the situation escalates into potential violence. OCA is eager to assist in the resolution of employee disputes and will not discipline employees for raising such concerns.

Employee Conduct & Disciplinary Action

Employee Conduct and Work Rules

To ensure orderly operations and provide the best possible work environment, OCA expects employees to follow rules of conduct that will protect the interests and safety of all employees and the organization.

It is not possible to list all the forms of behavior that are considered unacceptable in the workplace. The following are examples of infractions of rules of conduct that may result in

- Theft or inappropriate removal or possession of property;
- Falsification of timekeeping records;
- Working under the influence of alcohol or illegal drugs;
- Possession, distribution, sale, transfer, or use of alcohol or illegal drugs in the workplace, while on duty, or while operating employer-owned vehicles or equipment;
- Fighting or threatening violence in the workplace;
- Boisterous or disruptive activity in the workplace;
- Negligence or improper conduct leading to damage of employer-owned or customer-owned property;
- Insubordination or other disrespectful conduct;
- Violation of safety or health rules;
- Sexual or other unlawful or unwelcome harassment;
- Possession of dangerous or unauthorized materials, such as explosives or firearms, in the workplace;
- Excessive absenteeism or any absence without notice;

disciplinary action, up to and including termination of employment:

- Unauthorized use of telephones, mail system, or other employer-owned equipment;
- Unauthorized disclosure of business "secrets" or confidential information;
- Violation of personnel policies;
- Unsatisfactory performance or conduct.

Sexual and Other Unlawful Harassment

OCA is committed to providing a work environment that is free from all forms of discrimination and conduct that can be considered harassing, coercive, or disruptive, including sexual harassment. Actions, words, jokes, or comments based on an individual's sex, race, color, national origin, age, religion, disability, or any other legally protected characteristic will not be tolerated.

Sexual harassment is defined as unwanted sexual advances, or visual, verbal, or physical conduct of a sexual nature. This definition includes many forms of offensive behavior and includes gender-based harassment of a person of the same sex as the harasser. The following is a partial list of sexual harassment examples:

- Unwanted sexual advances;
- Making or threatening reprisals after a negative response to sexual advances;
- Visual conduct that includes leering, making sexual gestures, or displaying of sexually suggestive objects or pictures, cartoons or posters;
- Verbal conduct that includes making or using derogatory comments, epithets, slurs, or jokes;
- Verbal sexual advances or propositions;
- Verbal abuse of a sexual nature, graphic verbal commentaries about an individual's body, sexually degrading words, or suggestive or obscene letters or invitations;
- Physical conduct that includes touching, assaulting, or impeding or blocking movements.

Unwelcome sexual advances (either verbal or physical), and other verbal or physical conduct of a sexual nature constitute sexual harassment when:

(1) submission to such conduct is made either explicitly or implicitly a term or condition of employment;
(2) submission or rejection of the conduct is used as a basis for making employment decisions; or,
(3) the conduct has the purpose or effect of interfering with work performance or creating an intimidating, hostile, or offensive work environment.

If you experience or witness sexual or other unlawful harassment in the workplace, report it immediately to your supervisor. If the supervisor is unavailable or you believe it would be inappropriate to contact that person, you should immediately contact the Human Resource Department or any other member of management. You can raise concerns and make reports without fear of reprisal or retaliation.

All allegations of sexual harassment will be quickly and discreetly investigated. To the extent possible, your confidentiality and that of any witnesses and the alleged harasser will be protected against unnecessary disclosure. When the investigation is completed, you will be informed of the outcome of the investigation.

Any supervisor or manager who becomes aware of possible sexual or other unlawful harassment must immediately advise the Human Resource Department or any member of management so it can be investigated in a timely and confidential manner. Anyone engaging in sexual or other unlawful harassment will be subject to disciplinary action, up to and including termination of employment.

Personal Appearance

Dress, grooming, and personal cleanliness standards contribute to the morale of all employees and affect the business image OCA presents to visitors.

During business hours or when representing OCA, you are expected to present a clean, neat, and tasteful appearance. You should dress and groom yourself according to the requirements of your position and accepted social standards. This is particularly true if your job involves dealing with visitors in person.

Your supervisor or department head is responsible for establishing a reasonable dress code appropriate to the job you perform. Consult your supervisor if you have questions as to what constitutes appropriate appearance. Where necessary, reasonable accommodation may be made to a person with a disability.

Without unduly restricting individual tastes, the following personal appearance guidelines should be followed:

- Jeans, Bermuda, T-shirt and shorts do not present appropriate professional attire;
- Unnaturally colored hair and extreme hairstyles, such as spiked hair and shaved heads, do not present an appropriate professional appearance;
- Offensive body odor and poor personal hygiene is not professionally acceptable;
- Facial jewelry, such as eyebrow rings, nose rings, lip rings, and tongue studs, is not professionally appropriate and must not be worn during business hours;
- Multiple ear piercings (more than one ring in each ear) are not professionally appropriate and must not be worn during business hours.

Return of Property

Employees are responsible for all OCA property, materials, or written information issued to them or in their possession or control. Employees must return all OCA property immediately upon request or upon termination of employment. Where permitted by applicable laws, OCA may withhold from the employee's check or final paycheck the cost of any items that are not returned when required. OCA may also take all action deemed appropriate to recover or protect its property.

Resignation

At OCA, we understand that employees may choose to resign for a variety of reasons, and we strive to make the process as smooth and professional as possible.

If an employee chooses to resign, he or she must provide a written resignation letter to their immediate supervisor at least 2 weeks in advance. The letter must include the reason for resignation and the employee's intended last day of work. The supervisor will forward the letter to the HR department for record keeping.

During the notice period, the employee is expected to fulfill all their job duties and responsibilities in a professional manner. If the employee fails to do so, OCA reserves the right to immediately terminate the employee's employment without further notice.

Upon the employee's last day of work, the employee must return all company property, including but not limited to keys, access cards, and equipment, to their supervisor or HR department.

OCA respects the decisions of employees to resign and appreciates their service to the company. We strive to provide a smooth and professional process for all employees who choose to leave the company, and we encourage open communication throughout the process.

Security Inspections

OCA wishes to maintain a work environment that is free of illegal drugs, alcohol, firearms, explosives, or other improper materials. To this end, OCA prohibits the possession, transfer, sale, or use of such materials on its premises. OCA requires the cooperation of all employees in administering this policy.

Desks, lockers, and other storage devices may be provided for the convenience of employees but remains the sole property of OCA. Accordingly, they, as well as any articles found within them, can be inspected by any agent or representative of OCA at any time, either with or without prior notice.

Progressive Discipline

The purpose of this policy is to state OCA position on administering equitable and consistent discipline for unsatisfactory conduct in the workplace. The best disciplinary measure is the one that does not have to be enforced comes from good leadership and fair supervision at all employment levels.

OCA own best interest lies in ensuring fair treatment of all employees and in making certain that disciplinary actions are prompt, uniform, and impartial. The major purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

Although employment with OCA is based on mutual consent and both the employee and OCA have the right to terminate employment at will, with or without cause or advance notice, OCA may use progressive discipline at its discretion.

Disciplinary action may call for any of four steps – verbal warning, written warning, suspension with or without pay, or termination of employment – depending on the severity of the problem and the number of occurrences. There may be circumstances when one or more steps are bypassed.

Progressive discipline means that, with respect to most disciplinary problems, these steps will normally be followed: a first offense may call for a verbal warning; a next offense may be followed by a written warning; another offense may lead to a suspension; and, still another offense may then lead to termination of employment.

OCA recognizes that there are certain types of employee problems that are serious enough to justify either a suspension, or, in extreme situations, termination of employment, without going through the usual progressive discipline steps.

While it is impossible to list every type of behavior that may be deemed a serious offense, the Employee Conduct and Work Rules policy includes examples of problems that may result in immediate suspension or termination of employment. However, the problems

listed are not all necessarily serious offenses, but may be examples of unsatisfactory conduct that will trigger progressive discipline.

By using progressive discipline, we hope that most employee problems can be corrected at an early stage, benefiting both the employee and OCA.

Problem Resolution

OCA is committed to providing the best possible working conditions for its employees. Part of this commitment is encouraging an open and frank atmosphere in which any problem, complaint, suggestion, or question receives a timely response from OCA supervisors and management.

OCA strives to ensure fair and honest treatment of all employees. Supervisors, managers, and employees are expected to treat each other with mutual respect. Employees are encouraged to offer positive and constructive criticism.

If employees disagree with established rules of conduct, policies, or practices, they can express their concern through the problem resolution procedure. No employee will be penalized, formally or informally, for voicing a complaint with OCA in a reasonable, business-like manner, or for using the problem resolution procedure.

If a situation occurs when employees believe that a condition of employment or a decision affecting them is unjust or inequitable, they are encouraged to make use of the following steps.

1. Employee presents problem to immediate supervisor after incident occurs. If supervisor is unavailable or employee believes it would be inappropriate to contact that person, employee may present problem to Human Resource Department or any other member of management.

2. Supervisor responds to problem during discussion or after consulting with appropriate management, when necessary. Supervisor documents discussion.

3. Employee presents problem to Human Resource Department if problem is unresolved.

4. Human Resource Department counsels and advises employee, assists in putting problem in writing and visits with employee's manager(s), if necessary.
5. Employee presents problem to the COO in writing.

6. The COO reviews and considers problem. The COO informs employee of decision and forwards copy of written response to Human Resource Department for employee's file. The COO has full authority to make any adjustment deemed appropriate to resolve the problem.

Not every problem can be resolved to everyone's total satisfaction, but only through understanding and discussion of mutual problems can employees and management develop confidence in each other. This confidence is important to the operation of an efficient and harmonious work environment and helps to ensure everyone's job security.

Procurement and Contract Policies and Procedures

Purpose

The purpose of the procurement and contract policies are to establish clear guidelines and procedures for managing vendor-related activities and ensuring compliance with regulatory requirements. These policies aim to streamline the vendor selection process, maintain a reliable vendor database, and mitigate risks associated with vendor performance and contractual obligations. Additionally, they seek to protect the organization's interests by implementing measures such as blacklisting non-compliant vendors, obtaining temporary and final insurance, and verifying the validity of vendors' commercial registrations. By setting forth these policies, the organization aims to promote transparency, fairness, and accountability in its vendor management practices and safeguard its financial and operational interests.

Policy

- General Policies:
    - Employees must ensure not to disclose confidential information to any unauthorized party, especially regarding tenders.
    - Employees facing independence issues or conflicts of interest should report such issues to their supervisors.
    - The Procurement and Contract Department should retain all original copies of contracts.
    - No single department or employee should be solely responsible for any business process from start to finish. Tasks and authorities should be appropriately distributed and separated between purchasing requests, completion, and payment processes.
    - Purchasing procedures should be conducted fairly, competitively, and transparently.

- Purchasing Plan:
    - The purchasing plan includes outlining the procurement intentions of the OCA for the upcoming year.
    - The planning of purchases begins at the start of each fiscal year, at least one month before the budget preparation.
    - The plan provides details of the planned purchases, including:
        - Goods/Services/Projects
        - Quantity required
        - Brief description of the procurement subject, which may include codes or descriptors indicating product quality and preferred suppliers.

- Cost Estimation:
    - Priority is given to approved projects (resource allocation) during the purchasing planning process.
    - The purchasing team is responsible for making efforts to reduce costs and additional administrative expenses by consolidating requirements/contracts whenever possible.
    - The purchasing team should assist other departments in determining the costs for the planned purchases.
    - The annual purchasing plan serves as a planning tool only and does not constitute an invitation for bids or proposals. It is not a commitment from departments to purchase the described goods/services/works.

- Purchasing Methods:
    - The Procurement and Contract department is responsible for selecting the most appropriate purchasing method to ensure better risk control, timely supply of goods, services, and works, and achieving efficiency.
    - The entity generally follows the principle of competition among suppliers to obtain the highest level of service at the best prices. For low-value and low-risk purchases, competitive tendering can be waived, and purchasing methods are implemented as follows:

        - Direct Purchase Order: The direct purchase process is used for goods and services with a value not exceeding 2,000 Kuwaiti Dinars.
        - Practice-Based Purchase Order: The practice-based approach is used for goods and services with a value exceeding 2,000 Kuwaiti Dinars, requiring at least three price quotations.
    - Direct purchase requests are accepted if the following conditions are met:
        - Specifications of the goods and services.
        - Price schedule template.
        - Delivery schedule.
        - Offer validity period.
    - All offers are documented through fax or email directed to the Procurement and Contract Department.

- Purchasing Orders:
    - All official purchasing transactions between the entity and suppliers are carried out through purchase orders.
    - Requesters from the requesting department must provide sufficient lead time before the expected delivery date to enable the purchasing team to fulfill their duties properly and obtain the required goods according to the specifications/requirements.
    - It is not permissible to split purchases and contracts into multiple transactions to purchase them in amounts less than the specified threshold if they can be purchased in a single transaction. However, this division may occur if the purchase or contracts of the same type and specifications are requested within a timeframe of 3 months.
    - Priority should be given to all existing vendors in the supplier database over new vendors until the qualifications of the new supplier are proven.
    - All purchase orders and transactions within the entity are conducted by the purchasing team.
    - Personal items are not allowed to be purchased by the purchasing team.
    - Prior approval of all purchase orders must be obtained before initiating the purchasing process.

- Comprehensive Blanket Release (BR):
    - A Comprehensive Blanket Release (BR) is an order based on a contractual agreement called a Blanket Agreement (BA). The Blanket Agreement is an
    - agreement with the supplier to provide goods and services over a predetermined period of time and at predetermined prices. This practice aims to reduce the number of small orders and utilize short-term releases to meet the demand. Therefore, the Blanket Agreement is a contract between the entity and the preferred vendor for:
        - Repeated goods or services from the same vendor within a one-year period.
        - Orders for materials or supplies that require multiple shipments.
        - The entity obtains more competitive prices through commitments to specific purchase quantities or volume.
        - As a result of multiple procurement requests (such as IT equipment, consulting services, stationery, etc.), the Blanket Agreement helps bypass lengthy procedures that occur when requesting the same goods/services during the term of this agreement. All comprehensive agreements include the following information:
            - Timeframe (not exceeding one year unless business justification is clear or commitment for multiple years is warranted).
            - Included items and/or categories.
            - Minimum and maximum quantities, if applicable.
            - Prices.
            - Payment terms.

- Emergency Purchases:
    - Emergency purchases are allowed only under specific and justified circumstances.
    - Emergency purchase orders follow the same procedures as regular purchase orders, but with expedited review and approvals.
    - Purchases in emergency cases (goods/services/works) are those that meet the following conditions:
        - They may pose a risk to safety and public interest.

        - They occur due to unforeseen circumstances that cannot be avoided through proper planning and may cause significant financial loss or damage to the entity's reputation.
        - There is a need for a quick decision where time plays a critical role in resolving the problem.
    - All emergency purchase orders are sent to the Procurement and Contract Department, which reviews the nature of the purchase according to the aforementioned conditions and obtains approvals.

- Procurement and Contracting:
    - The Procurement and Contract Department is responsible for monitoring contracts and agreements.
    - Purchasing operations for goods and services with a value exceeding 2000 Kuwaiti dinars are conducted through tenders and contracts.
    - Before issuing any tender, approvals associated with it must be obtained.
    - The Procurement and Contract department is responsible for selecting the appropriate tendering method based on the requirements of the relevant departments, as follows:
        - Open tender, which is an open tender for all suppliers to submit their bids, announced in the official newspaper and OCA's website.
        - Limited tender, which is a closed tender applied when requesting bids from specific suppliers (who have already met pre-qualification requirements) or in cases where time constraints prevent following the open tender process. At least three suppliers are selected from the supplier database.
        - Single/sole sourcing, where a bid is requested from a single supplier who is preferred in terms of quality and service provided, or in cases where only one supplier is capable of providing a specific good/service in the market (such as an exclusive agent). Evidence must be provided that efforts have been made to communicate/identify other vendors offering the same goods and services. When resorting to single sourcing, approvals must be obtained.

- When announcing or issuing a tender, the tender documents must include the following:
  - Tender number, subject, and duration (tender announcement).
  - Scope of work, services, or required goods.
  - Tender documents and their price.
  - Instructions to bidders and general conditions.
  - Bid form.
  - Temporary insurance form.
  - Final insurance form.
- The Procurement and Contract Department is the central entity responsible for receiving all bids (physical and electronic documents, if applicable).
- The technical bids are evaluated by the Contracts and Tenders Committee in the presence of representatives from the relevant department, based on the specified procedure in the tender and the requirements of the concerned department.
- The commercial evaluation is conducted for bids that have successfully undergone the technical evaluation. In the case of multiple bids achieving the same result in the technical evaluation, the bid with the lowest price is selected.
- Contracts should be awarded based on competitive prices and the best value for money. However, in exceptional circumstances that must be documented, justified, and approved in writing, the entity may award the contract to a supplier other than the one offering the lowest price. Factors to be considered include quality, service performance, delivery, maintenance, and operation. The main objective in such circumstances is to achieve the most economically beneficial offer for the entity in the long term. Such decisions are made based on the recommendations of the Contracts and Tenders Committee.
- The Procurement and Contract Department is responsible for informing the supplier of their selection to provide the services or goods, and confirmation of acceptance must be obtained from the supplier within 7 working days from the date of notification.
- Notification of regret is sent to the other suppliers after signing the contract with the selected supplier.

- The Procurement and Contract department is responsible for drafting contracts and agreements with suppliers

- Supplier Management:
  - The Procurement and Contract Department is responsible for establishing qualification criteria for suppliers and creating/updating a database of qualified suppliers.
  - A supplier must be qualified before entering into any transaction or commercial arrangement with the entity and must be registered in the approved supplier registry.
  - The procurement team is responsible for evaluating the performance of suppliers in the following cases:
    - Annually for suppliers who are awarded annual contracts with a value exceeding 2000 Kuwaiti dinars.
    - In cases of contract renewals.
    - Immediately upon receiving any complaints about service providers from within the entity and every 24 months in remaining cases.
  - The Procurement and Contract Department may include certain suppliers in the blacklist primarily due to poor performance or unethical/illegal practices. The Procurement and Contract department is responsible for monitoring the record of suppliers included in the blacklist on a quarterly basis.
  - The Procurement and Contract Department is also responsible for organizing annual and periodic review meetings with key suppliers to discuss strategic direction, upcoming changes, business reviews, etc.

- Supplier Claims and Disputes:
  - Any claim or dispute must primarily be based on contractual/legal grounds in order to be considered.
  - All claims or disputes that will be escalated to arbitration/legal proceedings should be reported to the Procurement and Contract Manager, in coordination with the Legal Advisory.
  - All claims or disputes that will be escalated to arbitration/legal proceedings must be managed by the entity in accordance with applicable laws.

  - In all cases where the dispute remains unresolved for more than ninety (90) days from the receipt of the claim, and where it is unlikely to be resolved, it will be treated as an arbitration/legal proceeding.
  - The Procurement and Contract Manager maintains a record of all claims submitted during the fiscal year. The report should be based on the information recorded in the entity's complaint database/registry.

- Supplier Registration and Qualification:
  - Continuous evaluation of suppliers/vendors with whom there is ongoing or yearly engagement.
  - It is in the entity's interest to ensure, to the extent possible, that the source of all goods/services is from the registered approved vendors' list in the supplier database.
  - Supplier registration criteria should be periodically updated and reviewed, and each procurement category should have specific registration and evaluation criteria if necessary.
  - Only the Procurement and Contract Manager is authorized to contact vendors during the vendor qualification (registration) phase. Direct communication between vendors and entity employees during the qualification phase is not allowed.
  - The Procurement and Contract Manager has the right to reject a vendor if the vendor attempts to unduly influence the qualification process for their own benefit.
  - All vendors are subject to the same treatment in accordance with the entity's guidelines and values.

- Management of Vendor Master Data:
  - The procurement team should be the sole point of contact with vendors from the vendor database for all direct orders.
  - Creation of new vendors or updating/changing vendor master data should be done after obtaining approval from the Procurement and Contract Manager.

- Vendors Listed in the Blacklist:
    - All vendors listed in the blacklist should be banned from participating in bidding for all organization purchases for a minimum period of one calendar year.
    - To include a vendor in the blacklist, sufficient justification and necessary evidence must be provided.
    - The following guidelines apply when including vendors in the blacklist:
        - During the competitive bidding stage, a vendor may be blacklisted for any of the following violations:
            - Submitting bids containing false information or presenting forged documents to influence the outcome of any stage in the bidding process.
            - Withdrawing or refusing to accept any decision without proper justification.
            - Documented attempts by the bidder to influence the bid outcome for personal gain.
            - Failing to participate continuously in 5 bids/tenders without providing a valid written reason or declaring insolvency or liquidation by the authorities.
            - During the delivery/execution stage, a vendor may be blacklisted for any of the following violations:
                - Slow progress in delivering goods and/or services/work.
                - Making multiple unverified claims and/or consistently behaving in a non-compliant manner or continuously refusing to follow guidelines or instructions that are proven to be within the scope of the business project and contractual arrangements.
                - Vendor's failure, due to their own error or negligence, to take action and commence work or performance within the specified notice period.
                - Undertaking subcontracting without prior written approval from the organization.

- Guarantees and Insurance:
    - Temporary Insurance:
        - All bidders must provide a valid temporary insurance for a period of not less than 4 months from the date of completing the bid. The bidder is not allowed to cancel or withdraw their bid during the validity period.
        - The amount of the insurance is determined by the Procurement and Contract Department before announcing the bid. The temporary insurance should not exceed 5% of the estimated bid value.
        - In case the awarded bidder fails to sign the contract or provide the final guarantee/performance bond, which may result in financial loss for the organization, the temporary insurance will be settled to mitigate the risks of this loss. Some exceptions may be granted after obtaining the necessary approval.
    - Final Insurance/Performance Guarantee:
        - The final insurance serves as a guarantee for the organization that the supplier will fulfill the services/deliver the goods.
        - Any awarded bidder must provide the final insurance (the percentage of the final insurance is mentioned in the tender documents and should not be less than 10% of the contract value) within 10 working days (if in Qatar) or 20 working days (if abroad) from the notification of the award decision.
        - For materials/goods/supplies, the final insurance should be valid for at least 90 calendar days (or as per the Procurement and Contract Department's decision) from the delivery date. As for machinery and equipment, the validity should cover the warranty period plus an additional 45 calendar days.
        - The validity of the bank guarantee for service contracts extends until the contract period expires.
        - It is important to ensure the receipt of the final insurance in the required format before approving any invoice from the vendor.
        - In case of the vendor's breach, based on the recommendation of the concerned department, the Finance Department will settle the

        - performance bond after obtaining approval from the Procurement and Contract Department.
        - Performance bonds should be returned within a period not exceeding 7 days after the project's completion.

- The Commercial Register:
    - All vendors, suppliers, bidders, and/or quoters providing goods, works, and services to the organization and residing in the State of Kuwait must submit a valid copy of the Commercial Register issued by the Kuwaiti Ministry of Economy and Trade. The Commercial Register should be licensed for providing relevant goods and services.
    - All vendors, suppliers, bidders, and/or quoters residing in foreign countries and providing goods, works, and services to the organization must submit a valid copy of the Commercial Register in addition to the necessary licenses for providing goods and services issued by the relevant authorities in those foreign countries.

Procedures

- Purchasing Plan:
    - The procurement team leader initiates the planning for procurement processes one month prior to budget preparation. They gather and estimate the departments' needs for goods, services, and works. Based on that, the team leader develops the annual procurement plan, which includes:
        - 6.1.1 Description of goods, services, and works.
        - 6.1.2 Expected quantities.
        - 6.1.3 Estimated time frames.
    - The Procurement and Contract Manager reviews the procurement plan and provides feedback for adjustments to the team leader when necessary. Additionally, the plan is submitted to the authorized personnel for review and final approval.

- The authorized personnel, review the procurement plan and provide feedback for adjustments to the team leader when necessary. They approve the plan and inform the team leader accordingly.
- Upon receiving notification of the approved procurement plan, the team leader updates the list of items that require modification according to the approved plan. They add items to the list and define the plan in the system as needed. In all cases, the team leader must coordinate with the finance department to determine the relevant budgets. During the plan execution, the team leader is required to conduct periodic monitoring and prepare a report on any discrepancies.
- The Procurement and Contract Manager reviews the discrepancies and proposes corrective actions, which are then submitted to the authorized personnel for review and approval.
- The authorized personnel, review the proposed actions, secure the necessary approvals, and subsequently, the team leader updates the procurement plan according to the approved actions

- Supplier Management:

  - Based on the department's needs and the list of potential suppliers, the procurement team leader prepares requests for expressions of interest or requests for information from the suppliers. The requests for expressions of interest or requests for information serve as invitations to suppliers to provide the necessary information for inclusion in the approved suppliers list. The information that suppliers are required to provide includes, but is not limited to, the following: supplier's name and details, qualifications, offers, and services provided.
  - The Procurement and Contract Manager sends requests for information or expressions of interest to the specified suppliers and reviews the suppliers' responses to verify their compliance with the required eligibility criteria.
  - The Procurement and Contract Manager reviews the list of suppliers and their qualifications, prepares an apology letter, and sends it to the supplier in case they do not meet the eligibility criteria. In addition, the department head/lead sends qualification letters to the suppliers requesting them to

- provide registration data, including commercial registration, authorized signatories, contact information, and address.
- Based on the information received from the suppliers, the Procurement and Contract Manager registers the qualified supplier in the system and notifies the Financial Department of the new supplier registration.
- The Procurement and Contract Manager receives the supplier's claim notice and verifies the claim with the relevant department. The following details should be considered:
    - The actual nature of the claim and the surrounding circumstances.
    - The reasons, justifications, and bases that suppliers believe entitle their claims.
    - The relevant specific provisions of the agreement or applicable law.
- If the claim is legitimate, the following procedures are carried out:
    - The Procurement and Contract Manager conducts a detailed evaluation of the claim, including an assessment of contractual items, cost and impact assessment. Coordination with the Legal advisory is necessary for any negotiations with the supplier.
    - The authorized approver, reviews the evaluation report and approves it. The department head/lead then presents the claim and notifies the supplier accordingly.
- If the claim is not legitimate, the following procedures are followed:
    - The Procurement and Contract Manager must notify the supplier of the results with justifications. If the supplier does not accept the results, the dispute is escalated to the relevant authority for coordination with the Legal Advisory to conduct negotiations. If negotiations fail, the Legal Advisory proceeds to arbitration through legal procedures.
- The Procurement and Contract Manager determines the technical evaluation criteria.
- The department head/lead and the procurement team leader conduct periodic evaluations of suppliers. The department head/lead prepares a supplier performance report and corrective actions, which may include recommended corrective measures against the supplier to resolve issues, raise or lower the supplier's rating, or place them on the blacklist.

- Once the recommended actions are approved, the department head/lead follows up on the actions with the concerned supplier. If the actions indicate performance improvement, the following procedures are followed:
    - The department head/lead updates the supplier's performance status in the list if the actions require raising the supplier's rating. Otherwise, the supplier's rating remains unchanged, and the evaluation of the supplier's performance continues periodically. They may be classified as A, B, or C.
- If the actions do not indicate performance improvement, the following procedures are followed:
    - The department head/lead updates the supplier's status in the supplier list and initiates the process of "placing the supplier on the blacklist" if necessary. Suppliers on the blacklist are not allowed to submit any bids related to the entity.
- After completing the "Supplier Performance Evaluation" process, the Procurement and Contract Manager prepares a request to place the supplier on the blacklisted suppliers' list for a period less than one year, for one year, for a period exceeding one year, or for an indefinite period based on the results of the supplier's performance evaluation.
- The Procurement Team Leader sends a notification letter to the concerned supplier regarding their placement on the blacklisted suppliers' list. The content of this letter may vary from one supplier to another and provides a detailed explanation of the reasons for the decision to blacklist the supplier, along with clarifying the consequences of such a decision.
- Afterward, the team leader changes the supplier's status in the system to "Inactive Supplier." The system records the supplier as "Blacklisted Supplier," and the Procurement Team Leader is automatically notified when any of the blacklisted suppliers attempt to submit a qualification request through the official website. Such requests are considered invalid.
- It is the responsibility of the Procurement and Contract Manager to send the notification letter to the concerned supplier, explaining the reasons for their placement on the blacklisted suppliers' list. Additionally, the relevant department should be informed about the supplier's blacklisting status.

- Purchasing Orders
    - The Procurement and Contract Manager receives requests for goods or services or determines the need to issue a purchase order. Based on that, they enter the purchase request data into the system.
    - The Procurement and Contract Manager reviews the details of the request and approves it. If not approved, the department head/lead notifies the relevant department of the request rejection along with providing the justification.
    - Once approved, the Procurement and Contract Manager verifies the purchase request according to the procurement plan and ensures the availability of sufficient budget. They also coordinate with the Financial Department regarding any budget variances if the purchases are outside the budget. In addition, the required budget is reserved in the system.
    - The administrative services department employee must determine whether the required goods and services are covered by an existing contract. If they are covered, the employee should proceed with executing the purchase request and issuing a purchase order in accordance with the general contract. Otherwise, they obtain the detailed needs and specifications from the relevant department.
    - The Procurement and Contract Manager reviews the detailed requirements and determines the most suitable procurement method. They obtain the necessary approvals, selecting the procurement method in line with the approved purchasing policies, taking into consideration the value and nature of the required goods and services.
    - The authorized personnel, reviews the request for goods and services, as well as the specified procurement method. They inform the department head/lead to initiate the "tender request/ quotation request" when necessary. Otherwise, they notify the requester with the justifications.
    - If the process requires a request for quotations, the procurement officer prepares a quotation request in line with the purchasing policies. The request is then submitted for approval, followed by sending it to eligible suppliers. If the process requires a tender submission, the officer prepares the tender submission request and defines the tender submission criteria. It is then submitted to the Procurement and Contract Manager for review.

- The Procurement and Contract Manager reviews the tender submission request and criteria. They provide their feedback for any necessary modifications. Additionally, the department head/lead sends the request to the authorized personnel for approval.
- The authorized personnel, reviews the request and the submission criteria. They notify the Procurement and Contract Manager of the request rejection along with providing the justification, if applicable.
- In case of approval, the officer prepares the tender document and specifies its details in the system. The department head/lead announces the tender publicly or selects from a pre-qualified suppliers list. They also send the tender documents to potential suppliers.
- The officer receives bids from suppliers and forwards the temporary guarantee to the finance department if necessary.
- The Contracts and Tenders Committee evaluates the technical bids according to the evaluation criteria and selects the winning bids among them.
- Based on the committee's evaluation, the procurement team leader prepares the technical evaluation report. Then, the committee reviews the commercial bids and recommends the supplier selection.
- The procurement team leader prepares the comprehensive evaluation report and recommendations, which are submitted to the committee for review.
- The procurement and contract department conducts negotiations with the suppliers and documents the results in the report if necessary. Otherwise, the department prepares its final recommendation and awards the contract.
- The authorized personnel, reviews the evaluation report and recommendations, providing their feedback for any necessary modifications. Additionally, the procurement team leader prepares the contract award letter and proceeds with the "contract award" process.
- After conducting the tender evaluation, the Procurement and Contract team obtains approval for the selected bidder to issue the award letter. The award letter should be drafted in coordination with the relevant departments.

- The team requests the supplier to provide the final insurance and submits the document for signature.
- Subsequently, the team prepares the contract document and submits it for review and approval.
- The authorized personnel, review the contract document and provide their comments for necessary modifications. Once approved, the team sends two copies to the supplier for signing.
- Additionally, the team must inform unsuccessful suppliers and request the Finance department to release the temporary insurance bonds. They should also ensure that the contract and related files are archived.
- The Procurement team prepares purchase orders based on approved purchase requests and submits them to the Procurement and Contract Manager for review.
- The Procurement and Contract Manager reviews the purchase order details and obtains approval.
- The authorized personnel, review the purchase orders and provide their comments for necessary adjustments to the department head/lead. Apart from that, they authorize the purchase and inform the department head/lead, who then forwards the purchase order to the supplier and obtains an acknowledgment of receipt from the supplier.

Information Technology (IT) Policies and Procedures

Cyber Security Policy

This Cyber Security Policy includes guidelines and provisions for security measures to help mitigate cyber security risk. It applies to all organization employees, contractors, volunteers, and anyone who has permanent or temporary access to the organization's systems and hardware.

1. CONFIDENTIAL DATA

Confidential data is valuable and is to be kept secret. Organization confidential data includes:

- Unpublished financial information
- Data of employees/partners/vendors
- Patents, formulas or new technologies

All employees are obliged to protect this data.

2. PROTECT PERSONAL AND ORGANIZATION DEVICES

When employees use their digital devices to access organization emails or accounts, they introduce security risk to organization data. Employees are to keep both their personal and organization-issued computer, tablet and cell phone secure. To keep these devices secure:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Do not leave devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into organization accounts and systems through secure and private networks only.

Employees are advised to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive organization-issued equipment, they will receive instructions for:

- Disk encryption setup
- Password management tool setup
- Installation of antivirus/anti-malware software

Employees are to follow instructions to protect their devices and refer to organization Security Specialists/Network Engineers with any questions.

3. SAFEKEEPING EMAILS

Emails can host scams and malicious software. To avoid virus infection or data theft, employees must:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “Watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee isn’t sure that an email, they received is safe, they can refer to the organization Security Specialists.

4. MANAGING PASSWORDS

Password leaks are dangerous, since they can compromise the organization’s entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, employees are to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when necessary. When exchanging them in-person is

not possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every three months (90 days).

The organization will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

5. DATA TRANSFERS

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. financial data, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the organization's Security Specialists for help.
- Share confidential data over the organization network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Organization Security Specialists/Network Engineers need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our Security Specialists/Network Engineers, who must investigate promptly, resolve the issue and send an organization wide alert when necessary. Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

6. ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR Department.

- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in organization systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their organization equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.
Organization Security Specialists should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow these policies provisions as other employees do.

Our organization will have all physical and digital shields to protect information.

7. REMOTE EMPLOYEES

Remote employees must follow the Cyber Security Policy. As remote employees will be accessing the organization's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.
Remote employees are encouraged to seek advice from organization Security Specialists/IT Administrators.

8. DISCIPLINARY ACTION

All employees are to always follow this policy, and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: the organization may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): the organization will invoke more severe disciplinary action up to

and including termination.

Each incident will be examined on a case-by-case basis.
Additionally, employees who are observed to disregard the organization's security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

Data Security Policy

This Data Security Policy outlines behaviors expected of employees when dealing with Organization data. All forms of data are considered Organization assets. Shared information is a powerful tool and loss, or misuse can be costly, if not illegal. This Data Security Policy intends to protect the information assets of the organization.

In addition, in this Data Security policy, the main objective followed by OCA, is to establish and maintain adequate and effective data security measures for users, to ensure that the confidentiality, integrity and operational availability of information is not compromised.

Sensitive information must therefore be protected from unauthorized disclosure, modification, access, use, destruction or delay in service.

Each user has a duty and responsibility to comply with the information protection policies and procedures described in this document.

Purpose:
The purpose of this policy is to safeguard data and information belonging to OCA within a secure environment.

This policy informs OCA staff and other persons authorized to use OCA facilities of the principles governing the retention, use and disposal of information.

Scope:
This policy applies to all employees of OCA who use computer systems or work with documents or information that concerns customers, suppliers or any other partner for whom the organization has collected information in the normal course of its business.

1. GOALS AND OBJECTIVES FOLLOWED

The goals and objectives followed of this policy are:

- Protect information from unauthorized access or misuse;
- Ensure the confidentiality of information;
- Maintain the integrity of information;
- Maintain the availability of information systems and information for service delivery;
- Comply with regulatory, contractual and legal requirements;
- Maintain physical, logical, environmental and communications security;
- Dispose of information in an appropriate and secure manner when it is no longer in use;

2. AUTHORIZED USERS OF INFORMATION SYSTEMS

All users of OCA's information systems must be formally authorized by the Organization's Technology and IT Department. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

Authorized users shall take all necessary precautions to protect the OCA information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- the permission of the owner of the information;
- the risks associated with loss or falling into the wrong hands;
- how the information will be secured during transport to its destination.

3. ACCEPTABLE USE OF INFORMATION SYSTEMS

User accounts on the Organization's computer systems must only be used for the Organization's business and must not be used for personal activities during working hours.

- Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Organization systems for which they do not have authorization.

- Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the Organization IT designee. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Unauthorized use of the system may constitute a violation of the law, theft, and may be punishable by law. Therefore, unauthorized use of the Organization's computer system and facilities may constitute grounds for civil or criminal prosecution.

4. ACCESS CONTROL

The fundamental element of this Data Security policy is the control of access to critical information resources that require protection against unauthorized disclosure or modification.

Access control refers to the permissions assigned to persons or systems that are authorized to access specific resources. Access controls exist at different layers of the system, including the network. Access control is implemented by username and password. At the application and database level, other access control methods can be implemented to further restrict access.

Finally, application and database systems can limit the number of applications and databases available to users based on their job requirements.

5. NORMAL USER IDENTIFICATION

All users must have a unique username and password to access the systems. The user's password must remain confidential and under no circumstances should it be shared with management and supervisory staff and/or any other employees. Also, all users must comply with the following rules regarding password creation and maintenance:

- Password must not be found in any English or foreign dictionary. This means, do not use a common noun, verb, adverb or adjective. These can be easily cracked using standard "hacking tools";

- Passwords should not be displayed on or near computer terminals or be easily accessible in the terminal area;
- Password must be changed every 90 days;
- User accounts will be frozen after three failed logon attempts;
- Logon IDs and passwords will be suspended after 90 of days without use.

Below, you will find some additional important points to remember:

- Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.
- Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account.
- Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the Organization office.
- Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by (e.g. employee number) to the IT department.
- Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

6. CONFIDENTIALITY OF INFORMATION

Any information or documents that are not to be made public are designated as "Confidential Information". This information is invaluable to the Organization and therefore, all employees who, in the course of their duties, handle this type of information are expected to behave as follows:

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have a business "need-to-know."

- All electronic confidential information should be protected via firewalls, encryption and passwords.
- Employees should clear their desks of any confidential information before going home at the end of the day.
- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their workstations.
- All confidential information, whether contained on written documents or electronically, should be marked as "confidential."
- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)
- Employees should refrain from discussing confidential information in public places.
- Employees should avoid using e-mail to transmit certain sensitive or controversial information.
- Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver's license numbers) unless it is integral to the business transaction and restrict access on a "need-to-know' basis.
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

7. SECURITY OF INFORMATION

Information stored on computer systems must be regularly backed-up so that it can be restored if or when necessary.

All care and responsibility must be taken in the destruction of sensitive information. Electronic information relating to customers, administrative and commercial information must be disposed of in a secure manner.

Sensitive or confidential paper documents must be placed in the shredding bins or destroyed in the manner indicated to you by your department head.

8. USER RESPONSIBILITIES

Any data security system relies on the users of the system to follow the procedures necessary for upholding data security policies. Users are required to report any weaknesses in the Organization computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

Employees are therefore expected to:

- Comply with data security procedures and policies;
- Protect their user ID and passwords;
- Inform the Technology and IT Department of any data security questions, issues, problems or concerns;
- Assists the Technology and IT Department in solving data security problems;
- Ensures that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery;
- Be aware of the vulnerabilities of remote access and their obligation to report intrusions, misuse or abuse to the Technology and IT Department;
- Be aware of their obligations if they store, secure, transmit and dispose of vital information concerning the activities or operations of the Organization, customers, partners or strategic information on the Organization's products and services

9. MONITORING OF THE COMPUTER SYSTEM

The Organization has the right and capability to monitor electronic information created and/or communicated by persons using Organization computer systems and networks, including e-mail messages and usage of the Internet. It is not the Organization policy or intent to continuously monitor all computer usage by employees or other users of the Organization computer systems and network.

However, users of the systems should be aware that the Organization may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent

necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Organization policy.

10. SYSTEM ADMINISTRATOR

System administrators, network administrators and data security administrators will have access to the host systems, routers, hubs and firewalls necessary to perform their tasks.

All system administrator passwords will be deleted immediately after an employee who has access to these passwords has been terminated, dismissed or otherwise left the Organization's employment.

11. MANAGERS DUTY

Supervisors / Managers shall immediately and directly contact the Organization Technology and IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Incident Reporting and Escalation Policies and Procedures

Purpose:

The purpose of this policy is to define the process for reporting, managing, and escalating incidents that occur within the OCA network environment. This policy aims to ensure that incidents are handled promptly, efficiently, and effectively, minimizing the impact on the OCA organization.

Scope:

This policy applies to all employees, contractors, vendors, and any other parties who have access to OCA's network environment.

Policy:

1. Incident Reporting
   - 1.1 All incidents must be reported to the Technology & IT department as soon as possible.
   - 1.2 Incidents can be reported through various means, such as email, phone, or in-person.
   - 1.3 The report must include the following information:
     - 1.3.1 Date and time of the incident
     - 1.3.2 Description of the incident, including the impact on the system and data
     - 1.3.3 The individual(s) affected by the incident
     - 1.3.4 The location of the incident, if applicable
     - 1.3.5 Any other relevant information

2. Incident Management
   - 2.1 Upon receiving an incident report, the Technology & IT department will evaluate the severity of the incident and take appropriate actions.
   - 2.2 The Technology & IT department will assign an incident management team, consisting of appropriate members from IT, security, and other relevant departments.

2.3 The incident management team will analyze the incident, identify the root cause, and take necessary measures to mitigate the impact of the incident.
2.4 The incident management team will document all actions taken during the incident management process.

3. Incident Escalation
   3.1 Incidents will be escalated to higher management levels based on the severity of the incident and its potential impact on the OCA organization.
   3.2 The Technology & IT department will determine the level of escalation and the individuals who need to be informed.
   3.3 The incident management team will provide regular updates to the management and other stakeholders until the incident is resolved.
   3.4 If necessary, external authorities or agencies will be contacted to assist in the incident resolution.

4. Incident Communication
   4.1 The Technology & IT department will communicate incidents to all affected parties in a timely and appropriate manner.
   4.2 The incident communication will include the following information:
      4.2.1 The nature and severity of the incident
      4.2.2 The impact of the incident on the system and data
      4.2.3 Any actions that the affected parties should take to minimize the impact
      4.2.4 Any relevant updates and status reports
      4.2.5 Contact information for incident-related queries

Procedures:

1. Incident Reporting
   1.1 Upon discovering an incident, the individual must report it immediately to the Technology & IT department.
   1.2 If reporting through email or phone, the individual must provide all necessary information as listed in the policy section.

2. Incident Management

2.1 The Technology & IT department will evaluate the severity of the incident and assign an incident management team.

2.2 The incident management team will analyze the incident, identify the root cause, and take necessary measures to mitigate the impact of the incident.

2.3 The incident management team will document all actions taken during the incident management process.

3. Incident Escalation

3.1 The Technology & IT department will determine the level of escalation and the individuals who need to be informed.

3.2 The incident management team will provide regular updates to the management and other stakeholders until the incident is resolved.

3.3 If necessary, external authorities or agencies will be contacted to assist in the incident resolution.

4. Incident Communication

4.1 The Technology & IT department will communicate incidents to all affected parties in a timely and appropriate manner.

4.2 The incident communication will include the following information as listed in the policy section.

5. Incident Review

5.1 After the incident is resolved, an incident review will be conducted to assess the effectiveness of the response and identify any opportunities for improvement.

5.2 The incident review will be led by the Incident Manager, and may involve representatives from IT, security, legal, human resources, and any other relevant departments.

5.3 The incident review will evaluate the following:

5.3.1 The effectiveness of the response and whether it aligned with the incident response plan.

5.3.2 The root cause(s) of the incident.

5.3.3 Any areas where the incident response plan can be improved.

5.3.4 Any additional controls or training needed to prevent similar incidents in the future.

5.4 After the incident review is completed, a report will be prepared and shared with relevant stakeholders, including senior management and the Incident Response Team.

6. Escalation

6.1 Incidents may be escalated if they cannot be resolved by the Incident Response Team, or if they meet certain criteria defined in the incident response plan.

6.2 Escalation may involve notifying senior management, legal, external authorities, or other relevant parties, depending on the nature and severity of the incident.

6.3 The Incident Manager will be responsible for determining when escalation is necessary and coordinating the escalation process.

6.4 All relevant parties will be kept informed of the incident and the escalation process, as appropriate.

7. Training and Awareness

7.1 All employees, contractors, and third-party vendors with access to OCA's systems and data will receive regular training on the incident reporting and escalation procedures.

7.2 The training will cover:

7.2.1 The importance of timely and accurate incident reporting.

7.2.2 The escalation process and who to contact in the event of an incident.

7.2.3 The role of each team member in the incident response process.

7.3 In addition to training, OCA will maintain an awareness program to keep employees informed of the latest threats, vulnerabilities, and best practices for incident prevention and response.

8. Compliance Monitoring

8.1 OCA's Incident Response Team will conduct periodic reviews of incident reports and the incident response process to ensure compliance with this policy and other relevant policies and regulations.

8.2 Any identified non-compliance issues will be addressed promptly, and appropriate corrective actions will be taken.

8.3 The Incident Response Team will report on compliance monitoring activities to senior management and the Information Security Committee.

9. Policy Review and Maintenance

9.1 This policy will be reviewed annually, or more frequently as necessary, to ensure it remains effective and up-to-date.

9.2 The Incident Response Team will be responsible for recommending updates to this policy, as needed, based on changes in the threat landscape, regulatory requirements, or OCA's business operations.

9.3 This policy and related procedures will be maintained in a central location and accessible to all employees, contractors, and third-party vendors with access to OCA's systems and data.

Privacy Policies and Procedures

Purpose:

The purpose of this policy is to establish guidelines for protecting the privacy of personal information collected, processed, stored, transmitted, and/or disclosed by the OCA organization.

Scope:

This policy applies to all OCA employees, contractors, consultants, and third-party service providers who handle personal information on behalf of the organization.

Policy:

1. Collection of Personal Information
   - 1.1 Personal information should only be collected when necessary for legitimate business purposes.
   - 1.2 Individuals should be informed of the purposes for which their personal information is being collected, and consent should be obtained for its use.
   - 1.3 Personal information should only be collected from individuals directly or from other sources with their consent.

2. Use of Personal Information
   - 2.1 Personal information should only be used for the purposes for which it was collected.
   - 2.2 Personal information should not be disclosed to third parties without the individual's consent, except where required by law.
   - 2.3 Personal information should not be used for marketing purposes without the individual's consent.

3. Disclosure of Personal Information
   3.1 Personal information should only be disclosed to third parties when necessary for legitimate business purposes or as required by law.
   3.2 Third-party service providers who handle personal information on behalf of OCA must provide assurances that they will protect the privacy of the information.

4. Security of Personal Information
   4.1 Personal information must be protected by reasonable security safeguards against loss, theft, and unauthorized access, use, disclosure, or modification.
   4.2 Employees, contractors, consultants, and third-party service providers who handle personal information must be trained on the proper handling of such information.
   4.3 Incidents involving the unauthorized access, use, disclosure, or modification of personal information must be reported to OCA IT immediately.

5. Access to Personal Information
   5.1 Individuals have the right to access their personal information held by OCA.
   5.2 OCA must provide individuals with access to their personal information within a reasonable time and at no cost, except where permitted by law.
   5.3 Individuals may request that their personal information be corrected or updated if it is inaccurate or incomplete.

6. Retention of Personal Information
   6.1 Personal information should only be retained for as long as necessary to fulfill the purposes for which it was collected or as required by law.
   6.2 Personal information should be securely disposed of once it is no longer needed.

Procedures:

1. Collection of Personal Information

1.1 Personal information should only be collected when necessary for legitimate business purposes.
1.2 Individuals should be informed of the purposes for which their personal information is being collected, and consent should be obtained for its use.
1.3 Personal information should only be collected from individuals directly or from other sources with their consent.

2. Use of Personal Information
   2.1 Personal information should only be used for the purposes for which it was collected.
   2.2 Personal information should not be disclosed to third parties without the individual's consent, except where required by law.
   2.3 Personal information should not be used for marketing purposes without the individual's consent.

3. Disclosure of Personal Information
   3.1 Personal information should only be disclosed to third parties when necessary for legitimate business purposes or as required by law.
   3.2 Third-party service providers who handle personal information on behalf of OCA must provide assurances that they will protect the privacy of the information.

4. Security of Personal Information
   4.1 Personal information must be protected by reasonable security safeguards against loss, theft, and unauthorized access, use, disclosure, or modification.
   4.2 Employees, contractors, consultants, and third-party service providers who handle personal information must be trained on the proper handling of such information.
   4.3 Incidents involving the unauthorized access and disclosure of personal information must be reported immediately to the OCA Privacy Officer and Technology & IT department.
   4.4 Personal information must be encrypted when transmitted over public networks and stored on portable devices such as laptops, USB drives, and smartphones.

4.5 Personal information must be retained only for as long as necessary to fulfill the purposes for which it was collected, unless required by law or otherwise authorized.

4.6 Personal information must be securely disposed of when it is no longer needed, in accordance with OCA's records retention and disposal policy.

4.7 OCA must maintain a record of all disclosures of personal information, including the purpose of the disclosure, to whom it was disclosed, and when it was disclosed.

4.8 OCA must provide individuals with access to their personal information upon request, and allow them to request corrections to any inaccuracies.

4.9 OCA must obtain individuals' consent before collecting, using, or disclosing their personal information, except where permitted by law.

4.10 OCA must comply with all applicable privacy laws and regulations, and regularly review and update its privacy policies and procedures to ensure they remain effective and up-to-date.

5. Privacy Incident Response

5.1 If a privacy incident occurs, the incident must be reported to the Data Protection Officer immediately.

5.2 The Data Protection Officer will investigate the incident, assess the impact and decide whether to escalate the matter to the relevant regulatory authorities.

5.3 The affected individuals will be notified in a timely manner in accordance with applicable laws and regulations.

5.4 OCA will conduct a review of the incident to identify any necessary improvements to the privacy program, policies, procedures or training.

6. Privacy Compliance

6.1 OCA will conduct regular reviews of its privacy program to ensure ongoing compliance with applicable laws and regulations.

6.2 OCA will maintain records of all processing activities and will cooperate with supervisory authorities during audits and inspections.

6.3 OCA will provide training to all employees and contractors who handle personal data.

7. Privacy Policy Review

7.1 This Privacy Policy will be reviewed on an annual basis to ensure its ongoing relevance and effectiveness.

7.2 Any changes to this Privacy Policy will be communicated to all employees and contractors.

7.3 The Data Protection Officer will be responsible for ensuring that this Privacy Policy is reviewed and updated as necessary.

Encryption Policies and Procedures

Purpose:

The purpose of this policy is to define the standards and procedures for data encryption to protect the confidentiality, integrity, and availability of sensitive information.

Scope:

This policy applies to all employees, contractors, and third-party vendors who have access to OCA data or information systems.

Policy:

1. Encryption Standards
   1.1 All sensitive information stored on OCA servers or transmitted over OCA networks must be encrypted using industry-standard encryption algorithms and protocols, such as AES, RSA, SSL, or TLS.
   1.2 All encryption keys must be stored securely and in compliance with OCA's key management policy.

2. Encryption Requirements
   2.1 All laptops, desktops, and other portable devices that contain sensitive information must have full disk encryption enabled.
   2.2 All mobile devices that access OCA networks or data must have encryption enabled.

2.3 All sensitive information transmitted over public networks, such as the internet, must be encrypted using SSL or TLS.

2.4 All backup data must be encrypted during transmission and storage.

3. Encryption Procedures

3.1 OCA IT will be responsible for implementing and managing the encryption technologies used to protect sensitive information.

3.2 Employees are responsible for properly encrypting sensitive information according to this policy.

3.3 All encryption keys must be stored in a secure location.

3.4 Access to encryption keys must be restricted to authorized personnel only.

3.5 Any suspected or confirmed breaches of encryption must be reported immediately to OCA IT.

4. Third-Party Encryption

4.1 All third-party vendors who have access to OCA data or information systems must use encryption to protect sensitive information.

4.2 All third-party vendors must provide documentation of their encryption standards and procedures to OCA IT for review and approval.

4.3 Any suspected or confirmed breaches of third-party encryption must be reported immediately to OCA IT.

5. Encryption Key Management

5.1 All encryption keys must be managed in accordance with OCA's key management policy.

5.2 All encryption keys must be changed regularly and when personnel with access to the keys leave OCA employment.

5.3 All encryption keys must be backed up and securely stored offsite.

5.4 All encryption key backups must be tested regularly to ensure their effectiveness.

6. Encryption Monitoring and Review

6.1 OCA IT will monitor the use of encryption to ensure compliance with this policy.

6.2 Encryption effectiveness will be reviewed regularly to ensure its effectiveness.

6.3 Any changes to encryption standards or procedures must be reviewed and approved by OCA IT.

Procedures:

1. Encrypting Sensitive Information
   1.1 All sensitive information must be identified and classified according to OCA's data classification policy.
   1.2 Employees must ensure that sensitive information is properly encrypted using industry-standard encryption algorithms and protocols before it is transmitted or stored.
   1.3 All laptops, desktops, and other portable devices must have full disk encryption enabled.

2. Managing Encryption Keys
   2.1 Access to encryption keys must be restricted to authorized personnel only.
   2.2 All encryption keys must be stored in a secure location.
   2.3 All encryption keys must be backed up and securely stored offsite.
   2.4 All encryption key backups must be tested regularly to ensure their effectiveness.

3. Third-Party Encryption
   3.1 All third-party vendors who have access to OCA data or information systems must use encryption to protect sensitive information.
   3.2 All third-party vendors must provide documentation of their encryption standards and procedures to OCA IT for review and approval.

4. Enforcement
   4.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
   4.2 Any third-party vendor found to have violated this policy may have their contract terminated.

4.3 Any employee or third-party vendor found to have deliberately or maliciously tampered with or disabled encryption controls may face legal action.

5. Review
   5.1 This policy will be reviewed annually by the Technology & IT department to ensure that it is still applicable and effective.
   5.2 Any necessary updates or revisions will be made promptly to reflect changes in technology, regulations, or business needs.
   5.3 All employees and third-party vendors will be notified of any updates or changes to this policy.

6. Training and Education
   6.1 All employees will receive training on this policy and the importance of encryption controls during onboarding and annually thereafter.
   6.2 All third-party vendors must be made aware of this policy and their responsibilities related to encryption controls before being granted access to OCA systems or data.

7. Exceptions
   7.1 Exceptions to this policy may be granted by the Technology & IT department on a case-by-case basis, with approval from senior management.
   7.2 Any exceptions must be documented and approved in writing before being implemented.

8. Compliance
   8.1 Any noncompliance with this policy must be reported immediately to the Technology & IT department.
   8.2 Any violations of this policy will be investigated promptly by the Technology & IT department and appropriate action will be taken.
   8.3 Any questions or concerns regarding this policy or its implementation should be directed to the Technology & IT department.

Vulnerability Management Policies and Procedures

Purpose:

The purpose of this policy is to establish procedures and guidelines for identifying, assessing, prioritizing, and mitigating vulnerabilities in the information systems of OCA.

Scope:

This policy applies to all information systems, including hardware, software, and networks, used by OCA.

Policy:

OCA is committed to ensuring the confidentiality, integrity, and availability of its information systems. To achieve this goal, OCA will implement a vulnerability management program to identify, assess, prioritize, and mitigate vulnerabilities that could be exploited by attackers.

Procedures

Vulnerability Identification:

- OCA will use automated vulnerability scanning tools to identify vulnerabilities in its information systems.
- OCA will conduct manual vulnerability assessments as necessary to identify vulnerabilities that cannot be identified through automated tools.
- OCA will use threat intelligence feeds and other sources of information to identify potential vulnerabilities that could be exploited by attackers.

Vulnerability Assessment

- OCA will assess the severity and likelihood of exploitation of each identified vulnerability.
- OCA will determine the potential impact of each vulnerability on the confidentiality, integrity, and availability of OCA's information systems.

Vulnerability Prioritization

- OCA will prioritize vulnerabilities based on their severity, potential impact, and likelihood of exploitation.
- OCA will use the following categories to prioritize vulnerabilities:
    - Critical: Vulnerabilities that could be exploited to compromise the confidentiality, integrity, or availability of OCA's information systems.
    - High: Vulnerabilities that could result in a significant impact on the confidentiality, integrity, or availability of OCA's information systems.
    - Medium: Vulnerabilities that could result in a moderate impact on the confidentiality, integrity, or availability of OCA's information systems.
    - Low: Vulnerabilities that could result in a minor impact on the confidentiality, integrity, or availability of OCA's information systems.

Vulnerability Mitigation

- OCA will develop and implement a mitigation plan for each identified vulnerability.
- The mitigation plan will include the following:
    - Timeline for mitigation.
    - Resources required for mitigation.
    - Roles and responsibilities for mitigation.
- OCA will regularly review the effectiveness of the mitigation plan and adjust it as necessary.

Vulnerability Reporting

- OCA will maintain a vulnerability register that includes a record of all identified vulnerabilities, their severity, potential impact, and status.
- The vulnerability register will be updated on a regular basis to reflect changes in the status of vulnerabilities.
- OCA will report vulnerabilities to the relevant stakeholders, including management, system owners, and security personnel, as appropriate.

Vulnerability Remediation Verification

- OCA will verify that all identified vulnerabilities have been remediated.

- The verification process will include the following:
    - Validation of the remediation plan.
    - Confirmation that the remediation has been completed.
    - Validation that the remediation has been effective.

Vulnerability Scanning

Regular vulnerability scans should be conducted to identify potential vulnerabilities in the OCA's systems and applications. Scans should be scheduled at regular intervals and should cover all devices and applications within the OCA's environment. Scans should also be conducted after any significant changes to the environment.

Vulnerability Remediation

Once vulnerabilities are identified, they should be prioritized based on the severity and the potential impact on the OCA's environment. A plan should be developed to remediate the vulnerabilities within an appropriate time frame, and the plan should be reviewed and updated regularly.

Patch Management

To ensure that vulnerabilities are remediated in a timely manner, patch management processes should be established. This includes regular patching of all operating systems, applications, and other software within the OCA's environment. Patches should be tested in a non-production environment before being applied to production systems.

Change Management

Vulnerability management processes should be integrated with the OCA's change management processes to ensure that any changes to the environment do not introduce new vulnerabilities or impact the effectiveness of existing vulnerability management controls.

Reporting and Metrics

Regular reporting and metrics should be established to track the effectiveness of the OCA's vulnerability management program. This includes metrics on the number and

severity of vulnerabilities identified, the time to remediation, and the success rate of remediation efforts. Reports should be shared with relevant stakeholders to ensure transparency and accountability.

Acceptable Use Policies and Procedures

Overview:

This Acceptable Use Policy governs the use and security of all information and computer equipment from OCA. It also covers the use of email, the internet, voice and mobile computing equipment.

This policy applies to all information, in any form, relating to the business activities of OCA worldwide, and to all information processed by OCA about other organizations with which it deals.

This policy also covers all IT and information communication facilities operated by or on behalf of OCA.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of OCA. These systems are to be used for business purposes in serving the interests of the Organization, and of our clients and customers in the course of normal operations.

OCA is committed to protecting his employees, partners and the Organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

It is the responsibility of every OCA computer user to know these guidelines, and to conduct their activities accordingly.

Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at OCA. These rules are in place to protect the employee and OCA. Inappropriate use exposes

OCA to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope:

This policy applies to employees, contractors, consultants, temporary workers and other workers of OCA, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by OCA.

It also applies to the use of information, electronic and computer equipment and network resources to conduct business activities or interact with internal networks and business systems, whether owned or leased by OCA, the employee or a third party.

All employees, contractors, consultants, temps and other workers of OCA and its subsidiaries are responsible for exercising judgment with respect to the appropriate use of information, electronic devices and network resources in accordance with OCA policies and standards and local laws and regulations.

1. INDIVIDUAL'S RESPONSIBILITY

Access to the OCA IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the OCA IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any OCA IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access OCA's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to OCA's IT systems or information.
- Attempt to access data that they are not authorized to use or access.

- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non - OCA authorized device to the OCA network or IT systems.
- Store OCA data on any non-authorized OCA equipment.
- Give or transfer OCA data or software to any person or organization. outside OCA without the authority of OCA.

Line managers must ensure that individuals receive clear directives on the extent and limits of their authority over computer systems and data.

2. INTERNET AND EMAIL

The use of the internet and email of OCA is intended for professional purposes. Personal use is permitted when it does not affect the individual's professional performance, does not in any way harm OCA, does not violate any terms and conditions of employment and does not place the individual or OCA in violation of legal or other obligations. All individuals are therefore responsible for their actions on the internet as well as when using email systems.

Individuals must not:

- Use the internet or email for harassment or abuse.
- Use blasphemies, obscenities or disrespectful remarks in communications.
- Access, upload, send or receive data (including images) that OCA considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or run a personal business.
- Use the internet or email to play.
- Use email systems in a way that could affect their reliability or efficiency, for example by distributing chain letters or spam.
- Place on the internet any information relating to OCA, modify any information concerning it or express any opinion on OCA, unless they are expressly authorized to do so.
- Send sensitive or confidential information that is not protected to the outside world.

- Use of unsolicited email originating from within OCA 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by OCA or connected via 's network.
- Forward business email to personal email accounts (for example, Gmail account).
- Make official commitments by internet or email on behalf of OCA, unless authorized to do so.
- Download copyrighted material such as music media files (MP3), films and videos (non-exhaustive list) without appropriate approval.
- In any way, violate copyright, database rights, trademarks or other intellectual property rights.
- Download any software from the internet without the prior consent of the IT department.
- Connect OCA devices to the internet using non-standard connections.

3. GENERAL USE OWNERSHIP

- OCA proprietary information stored on electronic and computing devices whether owned or leased by OCA, remains the sole property of OCA. You must ensure through legal or technical means that proprietary information is protected in accordance with the data protection standards.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of OCA proprietary information.
- You may access, use or share OCA proprietary information only to the extent it is authorized and necessary to perform the tasks assigned to you.
- Employees are responsible for exercising their good judgment as to the reasonableness of personal use. It is the responsibility of each department to develop guidelines for the personal use of internet/intranet/extranet systems. In the absence of such policies, employees should be guided by their department's policies on personal use and, in the event of uncertainty, should consult their supervisor or manager.
- OCA reserves the right to periodically audit networks and systems to ensure compliance with this policy.

4. BLOGGING AND SOCIAL MEDIA

- Blogging by employees, whether using OCA's property and systems or personal computer systems, is also subject to the terms and restrictions set out in this policy. The limited and occasional use of OCA systems for blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate OCA policy, does not prejudice the best interests of OCA and does not interfere with the employee's normal duties. Blogging from OCA 's systems are also subject to monitoring.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of OCA and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
- Employees may also not attribute personal statements, opinions or beliefs to OCA when engaged in blogging.

5. SECURITY AND PROPRIETARY INFORMATION

- All access to the Organization's computer network must be protected by passwords.
- It is prohibited to allow access to another person, either deliberately or by failing to adequately protect the right of access that has been granted.
- All computer devices shall be protected by a password-protected screen saver with an automatic activation function set to 10 minutes or less. You must lock the screen or disconnect when the unit is unattended.
- Messages posted by employees from and OCA email address on forums should contain a warning that the opinions expressed are strictly theirs and not necessarily those of OCA, unless the message is posted in the course of professional duties.
- Employees must exercise extreme caution when opening attachments to emails received from unknown senders, which may contain malware.
- Employees must not remove or disable anti-virus software.

- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved OCA anti-virus software and procedures.

6. WORKING OFF SITE

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with OCA remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely. Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as USB flash drives, CDs, DVDs and removable hard drives should only be used when network connectivity is not available or there is no other secure method of data transfer. Only authorized OCA mobile storage devices with encryption enabled should be used when transferring sensitive or confidential data.

Software

Employees shall use only software that is authorized by OCA on OCA’s computers. Authorized software must be used in accordance with the software supplier's licensing

agreements. All software on OCA computers must be approved and installed by the OCA IT department.

7. UNACCEPTABLE USE

The following activities are prohibited. Under no circumstances is an employee of OCA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing OCA-owned resources.
The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Infringements of the rights of any person or Organization protected by copyright, trade secret, patent or other intellectual property, or by similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" products or other software the use of which is not authorized by OCA.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OCA or the end user holds no active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Making fraudulent offers of products, items, or services originating from any OCA account.
- Making security breaches or disruptions of network communication.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, employees to parties outside OCA.

Backup Policies and Procedures

To meet the Organization's business objectives and ensure continuity of its operations, OCA (the "Organization") shall adopt and follow well-defined and time-tested plans and procedures, to ensure timely and reliable backup of its IT assets. The Backup Policy reiterates the commitment of the Organization towards delivering the fastest transition and highest quality of services through the backup arrangement, ensuring that its customers, business activities, and services do not suffer in any way.

Definitions:

- Backup. To copy data to a second location, solely for the purpose of safe keeping of that data.
- Backup Media. Any storage devices that are used to maintain data for backup purposes. These can be tapes, CDs, DVDs, or hard drives.
- Full Back up. A backup that makes a complete copy of the target data.
- Incremental Backup. A backup that only backs up files that have changed within a designated time period, typically since the last backup was run.
- Restoration. Also called "recovery." The process of restoring the data from its backup state to its normal state so that it can be used and accessed in a regular manner.

Purpose:

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

Scope:

This policy applies to all data stored on the Organization's systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

1. IDENTIFICATION OF CRITICAL DATA

The Organization must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

2. DATA TO BE BACKED UP

A Backup Policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to Organization operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s), as well as these servers' operating systems and logs. It is the users' responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers.
- Logs and configuration of network devices such as switches, routers, etc.
- Information stored on employee desktops if the backup administrator deems such information necessary and backup facilities exist for such an endeavor. The backup administrator may instead choose to back up a standard desktop configuration and restore data from the file server at his or her discretion.

3. BACKUP FREQUENCY

Backup frequency is critical to successful data recovery. The Organization has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Incremental: Daily basis
Full: Once a week

4. OFF-SITE ROTATION

Geographic separation from the backups must be maintained, to some degree, to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the Organization's uptime requirements. The Organization has determined that backup media must be rotated off-site at least once per week.
The off-site rotation strategy should be designed to store backup data in a secure and remote location, such as a different physical location or cloud-based storage.

5. BACKUP STORAGE

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, Organization data, precautions must be taken that are commensurate with the type of data being stored. The Organization has set the following guidelines for backup storage.

When stored onsite, backups should be kept in an access-controlled area. When shipped off-site, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including fire suppression, and security processes, must be used to ensure the integrity of the backup media. Online backups are allowable if the service meets the criteria specified herein.

6. BACKUP RETENTION

When determining the time required for backup retention, the Organization must determine what number of stored copies of backed-up data is sufficient to effectively

mitigate risk while preserving required data. The Organization has determined that the following will meet all requirements (note that the Backup Retention Policy must confirm to the Organization's Data Retention Policy and any industry regulations, if applicable): Incremental Backups must be saved for Four (4) weeks. Full Backups must be saved for Three (3) months.

7. RESTORATION PROCEDURES AND DOCUMENTATION

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not a) misinterpreted by readers other than the backup administrator, and b) confusing during a time of crisis.

8. RESTORATION TESTING

Since a Backup Policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year.

9. EXPIRATION OF BACKUP MEDIA

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service, the media can no longer be considered dependable. When backup media is put into service, the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

10. APPLICABILITY OF OTHER POLICIES

This document is part of the Organization's cohesive set of security policies. Other policies may apply to the topics covered in this document, and, as such, the applicable policies should be reviewed as needed.

11. ENFORCEMENT

This policy will be enforced by the Technology and IT Manager. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Organization property (physical or intellectual) are suspected, the Organization may report such activities to the applicable authorities.

Bring Your Own Device (BYOD) Policies and Procedures

This document provides guidelines for the use of personally owned smart phones and/or tablets by OCA employees (users) to access OCA network resources. The access and use of the network services is granted on condition that each user reads, signs, respects, and follows the OCA's policies concerning the use of these devices and services.

Purpose of this BOYD

OCA grants its employees the privilege of using their own smartphones and tablets, of their choice, at work for their convenience. This BYOD Policy is intended to protect the privacy, security and integrity of OCA 's data and technology infrastructure against the risks that can arise when employees use their personally owned devices for business purposes.

OCA employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the organization network.

OCA reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

1. BOYD DEVICES

The following devices are approved for employee BOYD use and connecting to the OCA network:

- Laptops
- Tablets
- Smartphones
- Portable storage devices

Before any access to organization's network, devices must be presented to IT department for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools.

2. PRIVACY

OCA will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device).

3. ACCEPTABLE USE

a) The organization defines acceptable business use as activities that directly or indirectly support the business of OCA.
b) The organization defines acceptable personal use on organization time as reasonable and limited personal communication or recreation, such as:
    - Occasional personal calls or texts during breaks or outside of work hours
    - Limited use of personal email or social media during breaks or outside of work hours
    - Use of personal devices during work hours for emergencies or urgent personal matters only
    - Limited use of non-work-related websites or apps during breaks or outside of work hours.
c) Employees may use their BYOD devices for the acceptable business and personal uses of OCA computers as set out in the OCA Computer Use Policy

    - Email
    - Calendar
    - Contact information
    - Document sharing and collaboration tools
d) The following apps are permitted for downloading, installation and use on BYOD devices

- Email and productivity apps, such as Gmail, Outlook, and Microsoft Office.
- Communication apps, such as Skype, Slack, and Zoom.

4. RESTRICTIONS

a) Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the organization. Such websites include but are not limited to:

- Social media websites, such as Facebook, Twitter, and Instagram.
- Entertainment websites, such as YouTube, Netflix, and Hulu.
- Shopping websites, such as Amazon and eBay.
- Gambling websites.
- Adult websites.
- Websites that contain malware or other security threats.
- Websites that are not related to work.

b) Employees may not use their BYOD devices during work hours for personal purposes that are not permitted for use of OCA computers as set out in the OCA Computer Use Policy, e.g., BYOD devices may not be used for accessing pornographic or offensive materials, storing or transmitting OCA proprietary information, committing harassment, engaging in business activities that are in conflict of interest with their duties to OCA, etc.

c) The following apps are not allowed for downloading, installation and use on BYOD devices.

- Apps that contain malware or other security threats.
- Apps that violate the organization's security policies.
- Apps that contain inappropriate content.

- Apps that are not related to work.
- Apps that are not approved by the organization's IT department.

d) OCA has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted

5. SENSITIVE DATA

User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or organization financial operations.

6. OBLIGATIONS

a) Not sharing their BYOD devices with friends, relatives or anybody other than a properly authorized user of the device under this BYOD Policy;
b) Using their BYOD devices to access only the information authorized for that employee to access under the OCA authentication and authorization procedures;
c) Reporting lost, misplaced or stolen BYOD devices to the IT department (and mobile carrier) within 24 hours;
d) Paying all costs associated with purchasing and their BYOD device.

7. SECURITY

a) Before accessing the OCA network, employees must present their BYOD devices to the IT department for task provisioning and configuration of standard applications, such as browsers, desktop productivity software and security tools.
b) In order to prevent unauthorized access to the organization's network, devices must be protected by a strong password before using the organization's network.
c) Follow the password policy (please review the password policy document).
d) The device must be locked with a password or PIN if it is inactive for 15 minutes.

e) After five unsuccessful connection attempts, the device must lock. Employees must then contact the IT department to retrieve access
f) Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
g) It is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
h) Employees are automatically prevented from downloading, installing and using any app that does not appear on the organization's list of approved apps.
i) Smartphones and tablets that are not on the organization's list of supported devices are not allowed to connect to the network.
j) Employees' access to organization data is limited according to user profiles defined by IT and automatically applied.
k) The employee's device can be remotely wiped if 1) the device is lost, 2) the employee leaves the organization, 3) the computer detects a data or policy violation, virus or similar threat to the security of the organization's data and technological infrastructure.

8. MISCELLANEOUS/DISCLAIMERS

a) The organization reserves the right to disconnect devices or disable services without notice.
b) Lost or stolen devices must be reported to the organization within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
c) Employees are expected to use their devices ethically at all times and to comply with the organization's acceptable use policy described above.
d) Employees are personally liable for all costs associated with their device.
e) OCA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Cloud Computing Policies and Procedures

Purpose:

The purpose of this policy is to outline the guidelines and responsibilities for the use of cloud computing services by employees and contractors of OCA.

Scope:

This policy applies to all employees and contractors of OCA who utilize cloud computing services.

Policy:

- Use of Cloud Computing Services: The use of cloud computing services by OCA employees and contractors must comply with all applicable laws, regulations, and policies of OCA. Cloud computing services must be used only for business-related purposes and authorized by management.
- Data Classification: All data stored on cloud computing services must be classified according to the OCA data classification policy.
- Data Backup and Recovery: OCA data stored on cloud computing services must be backed up and recoverable in the event of a disaster or system failure. Backup and recovery procedures must be documented and tested periodically.
- Security and Privacy: The security and privacy of OCA data stored on cloud computing services must be protected at all times. All cloud computing services must meet OCA security and privacy standards.
- Access Control: Access to cloud computing services must be restricted to authorized employees and contractors only. Access control procedures must be documented and reviewed periodically.
- Monitoring and Auditing: OCA must monitor and audit cloud computing services to ensure compliance with this policy, applicable laws, regulations, and policies of OCA.
- Service Level Agreements (SLAs): Cloud computing services must have an SLA that meets or exceeds OCA's requirements for availability, performance, and support. All SLAs must be reviewed and approved by OCA management.

- Termination of Services: OCA reserves the right to terminate any cloud computing service at any time, with or without notice.

1. Incident Response Procedures

- Approval Process: Requests for cloud computing services must be approved by management. The approval process should include an evaluation of the cloud computing security and privacy standards.
- Data Classification: All data stored on cloud computing services must be classified according to the OCA data classification policy.
- Backup and Recovery: Backup and recovery procedures must be documented and tested periodically.
- Security and Privacy: All cloud computing services must meet OCA security and privacy standards.
- Access Control: Access to cloud computing services must be restricted to authorized employees and contractors only. Access control procedures must be documented and reviewed periodically.
- Monitoring and Auditing: OCA must monitor and audit cloud computing services to ensure compliance with this policy, applicable laws, regulations, and policies of OCA.
- SLA Review: All SLAs must be reviewed and approved by OCA management.

Service Level Agreement for Cloud Computing Services

1. Service Description

The Cloud Computing Services (the “Services”) covered by this Service Level Agreement (“SLA”) are described in the Cloud Computing Policy of our organization. The Services provided shall include, but not be limited to, the following:

- Provision of cloud-based infrastructure, platform, software, and/or storage services
- Maintenance and support of the cloud environment
- Availability of technical support services to resolve issues or incidents

2. Service Availability

The cloud computing service will be available 99.99% of the time on an annual basis, excluding scheduled maintenance and force majeure events. Scheduled maintenance will be performed during a defined maintenance window, which shall not exceed eight (8) hours per month, and notice will be provided to the OCA's management in advance.

3. Performance Metrics

The following performance metrics shall apply to the Services:

- Response Time: The response time for critical issues or incidents shall be less than 15 minutes, with a goal of resolving the issue or incident within four (4) hours.
- Resolution Time: The resolution time for critical issues or incidents shall be less than four (4) hours, with a goal of resolving the issue or incident within 24 hours.
- Uptime: The uptime of the cloud environment shall be measured monthly and reported to the OCA's management.

5. Incident Management

The incident management process will include the following:

- Incident Reporting: incidents shall be reported via email or phone to the technical support team.
- Incident Tracking: The technical support team will track incidents and provide the OCA management with regular updates until the incident is resolved.
- Incident Resolution: The technical support team will resolve incidents based on the priority assigned and the resolution times outlined in this SLA.

6. Security

The technical support team will ensure the security of the cloud environment by implementing appropriate security measures and controls, including access controls,

firewalls, intrusion detection and prevention systems, and data encryption. The technical support team will also perform regular security audits and vulnerability assessments to ensure the security of the cloud environment.

7. Data Backup and Recovery

The technical support team will implement a data backup and recovery process to ensure the availability and recoverability of OCA data. The data backup and recovery process will include the following:

- Data Backup: The technical support team will perform regular backups of OCA data to ensure that data is recoverable in the event of data loss or corruption.
- Data Recovery: The technical support team will implement a data recovery process to restore OCA data in the event of data loss or corruption.

Data Classification Policies and Procedures

The purpose of this Data Classification Policy is to establish a framework for the classification of data owned or managed by the OCA. This policy is intended to provide guidance on the proper handling of data based on its sensitivity and value, and to ensure that appropriate security measures are implemented to protect it.

Definitions

- Confidential Information

  Information that is intended to be kept secret and is not publicly available. This includes personally identifiable information, financial information, intellectual property, and other sensitive data.
- Internal Information

  Information that is intended for internal use only and is not publicly available. This includes company policies, internal memos, and other internal communications.
- Public Information

  Information that is publicly available and does not contain sensitive or confidential information.

Purpose:

The purpose of this policy is to:

- Establish a framework for the classification of data based on its sensitivity and value.
- Ensure that appropriate security measures are implemented to protect data based on its classification.
- Provide guidance on the proper handling of data based on its classification.

Scope:

This policy applies to all data owned or managed by the OCA, including data stored on its systems and networks, data stored in the cloud, and data stored on mobile devices.

1. Roles and Responsibilities

Data Owner

The Data Owner is responsible for:

- Determining the sensitivity and value of data.
- Ensuring that appropriate security measures are implemented to protect data based on its classification.
- Ensuring that data is properly classified and labeled.

Data Custodian

The Data Custodian is responsible for:

- Implementing and maintaining appropriate security measures to protect data based on its classification.
- Ensuring that data is stored, transmitted, and processed in accordance with its classification.

Data User

The Data User is responsible for:

- Ensuring that they have the appropriate level of access to data based on its classification.
- Ensuring that they handle data in accordance with its classification.
- Reporting any suspected security incidents involving data.

2. Data Classification Categories

Data owned or managed by the Olympic OCA shall be classified into one of the following categories:

Confidential Information

Data that is intended to be kept secret and is not publicly available. This includes personally identifiable information, financial information, intellectual property, and other sensitive data. Confidential information shall be protected using the highest level of security measures.

Internal Information

Data that is intended for internal use only and is not publicly available. This includes company policies, internal memos, and other internal communications. Internal information shall be protected using appropriate security measures.

Public Information

Data that is publicly available and does not contain sensitive or confidential information. Public information may be freely accessed and shared.

3. Data Handling Guidelines

Confidential Information

Confidential information shall be handled in accordance with the following guidelines:

- Access to confidential information shall be restricted to those with a legitimate need-to-know.
- Confidential information shall be encrypted when stored and transmitted.
- Confidential information shall be labeled as such and stored in a secure location.
- Confidential information shall be destroyed in a secure manner when no longer needed.

Internal Information

Internal information shall be handled in accordance with the following guidelines:

- Access to internal information shall be restricted to those with a legitimate need-to-know.
- Internal information shall be labeled as such and stored in a secure location.
- Internal information shall not be shared with external parties without proper authorization.

Public Information

Public information shall be handled in accordance with the following guidelines:

- Public information may be freely accessed and shared.
- Public information shall be labeled as such and stored in a location accessible to the public.

Other Outlines

- Regular training shall be provided to all employees on the proper handling of data based

Email Policy (Strict)

This document sets forth the policy of OCA (the “Organization”) with respect to email. All employees who use the Organization’s email system are required to comply with this policy statement.

1. Business Use
   The email system is to be used solely for business purposes of the Organization and not for personal purposes of the employees.

2. Ownership
   All information and messages that are created, sent, received or stored on the Organization’s email system is the sole property of the Organization.

3. Email Review
   All email is subject to the right of the Organization to monitor, access, read, disclose and use such email without prior notice to the originators and recipients of such email. Email may be monitored and read by authorized personnel for the Organization for any violations of law, breaches of Organization policies, communications harmful to the Organization, or for any other reason.

4. Prohibited Content
   Emails may not contain statements or content that are libelous, offensive, harassing, illegal, derogatory, or discriminatory. Foul, inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited. Sexually explicit messages or images, cartoons or jokes are prohibited.

5. Security
   The email system is only to be used by authorized persons, and an employee must have been issued and email password in order to use the system. Employees shall not disclose their codes or passwords to others and may not use someone else’s code or password without express written authorization from the Organization.

6. No Presumption of Privacy
   Email communications should not be assumed to be private and security cannot be guaranteed. Highly confidential or sensitive information should not be sent through email.

7. Certain Prohibited Activities
   Employees may not, without the Organization's express written authorization transmit trade secrets or other confidential, private or proprietary information or materials through email.

8. Message Retention and Creation
   Employees should be careful in creating email. Even when a message has been deleted, it may still exist in printed version, be recreated from a back-up system, or may have been forwarded to someone else. Please note that appropriate electronic messages may need to be saved. And, the Organization may be required to produce email in litigation.

9. Viruses
   Any files downloaded from email received from non-Organization sources must be scanned with the Organization's virus detection software. Any viruses, tampering or system problems should be immediately reported to (computer systems administrator)

10. Consequences of Violations
    Violations of this policy or other organization policies may result in discipline, suspension and even termination of employment.

Help Desk Support Policies and Procedures

Purpose:

The purpose of the Help Desk Support Policy and Procedures is to establish guidelines for the effective and efficient provision of technology support services to all OCA users.

Scope:

This policy applies to all OCA employees, contractors, and other authorized users who require technology support services.

Policy:

The following policies should be followed by the Help Desk Support team to ensure effective and efficient technology support services:

1. Service Level Agreement:

The Help Desk Support team will adhere to a Service Level Agreement (SLA) that outlines the expected response time and resolution time for each type of support request. See the details of SLA in SLA-Policy-D2340.doc

2. User Authorization:

The Help Desk Support team will only provide support services to authorized users who have been granted access to OCA technology resources.

3. User Education and Awareness:

The Help Desk Support team will provide education and awareness materials to users to help them understand best practices for using OCA technology resources and to avoid common issues.

4. Data Privacy and Security:

The Help Desk Support team will maintain the privacy and security of user data at all times. This includes adhering to all OCA data privacy and security policies and procedures.

5. Incident Reporting:

The Help Desk Support team will report all incidents of security breaches, data loss, or other security incidents to the appropriate OCA teams as per OCA's incident management policies and procedures.

Procedures:

The following procedures should be followed by the Help Desk Support team to ensure efficient and effective technology support services:

1. Help Desk Support Hours:

The Help Desk Support team will provide support during the following hours: From Sunday to Thursday, 9:00AM till 3:00PM.

2. Help Desk Support Channels:

Users may contact the Help Desk Support team through the following channels:

- Phone: +965-22274277/88/99/
- Email: info@ocasia.org

3. Ticketing System:

The Help Desk Support team will use a ticketing system to track and manage all user requests for support. All requests for support should be logged into the ticketing system and assigned a unique ticket number.

4. Escalation Procedures:

Level 1: Help Desk staff

The help desk staff is the first point of contact for end-users who need assistance. They are responsible for triaging tickets and determining the appropriate level of

support. If the help desk staff can resolve the issue, they will do so. If the issue cannot be resolved, they will escalate the ticket to the next level of support.

Level 2: Technical Support staff
The technical support staff is responsible for resolving issues that are beyond the scope of the help desk staff. They may have access to more specialized tools and resources, and they may have more experience in resolving complex issues.

Level 3: External Vendors
In some cases, the issue may be so complex or specialized that it requires the assistance of an external vendor. In these cases, the technical support staff will work with the vendor to resolve the issue.

In the event that the Help Desk Support team is unable to resolve an issue, the escalation procedures below will be followed:

- The end-user creates a ticket and submits it to the help desk.
- The help desk staff triages the ticket and determines the appropriate level of support.
- If the help desk staff can resolve the issue, they will do so.
- If the help desk staff cannot resolve the issue, they will escalate the ticket to the next level of support.
- The technical support staff will work to resolve the issue.
- If the technical support staff cannot resolve the issue, they will escalate the ticket to an external vendor.
- The external vendor will work to resolve the issue.
- The help desk staff will keep the end-user updated on the status of the ticket.
- Once the issue is resolved, the help desk staff will close the ticket.

5. User Identification:

The Help Desk Support team will verify the identity of the user making the support request. This may include requesting the user's name, employee ID, or other identifying information.

6. Issue Triage and Resolution:

The Help Desk Support team will use a standardized triage process to determine the severity and priority of each support request. Requests will be prioritized based on the impact to the user and the organization. The team will work to resolve all issues as quickly as possible and will provide regular updates to the user throughout the process.

7. Communication and Follow-up:

The Help Desk Support team will maintain regular communication with the user throughout the support process. This includes providing regular updates on the status of the request and ensuring that the user is satisfied with the resolution.

8. Documentation and Reporting:

The Help Desk Support team will maintain accurate records of all support requests, including the date and time of the request, the issue reported, the steps taken to resolve the issue, and the resolution provided. The team will provide regular reports on support metrics to management.

9. Training:

The Help Desk Support team will undergo regular training to ensure they are equipped with the skills and knowledge to provide effective support. Training will include:

- Technical training: To keep the team updated on the latest technologies and tools used by the organization.
- Soft skills training: To help the team communicate effectively with users and manage end-user expectations.

- Process training: To ensure the team is familiar with the processes and procedures followed by the Help Desk Support team.

10. Feedback and Continuous Improvement:

The Help Desk Support team will seek feedback from users to identify areas for improvement. Feedback will be used to continuously improve the support provided by the team. The following methods will be used to collect feedback:

- Surveys: Periodic surveys will be conducted to gather feedback from users.
- User interviews: The Help Desk Support team will conduct user interviews to gather feedback and suggestions for improvement.

11. Compliance:

The Help Desk Support team will comply with all relevant policies and regulations. The following regulations will be adhered to:

- Data Protection Regulations: The Help Desk Support team will ensure that all user data is protected and handled in accordance with data protection regulations.
- IT Security Policies: The Help Desk Support team will comply with IT Security Policies to ensure the security of the organization's IT infrastructure and data.
- Industry Regulations: The Help Desk Support team will comply with any industry-specific regulations applicable to the organization.

Internet Policy

Policy:

OCA's (the "Organization" or "our" or "we") Internet Policy outlines the guidelines for using an internet connection, network, and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our organization's legality and reputation.

Purpose:

All internet data that is written, sent, or received through our computer systems is part of official OCA records. That means that we can be legally required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

The equipment, services, and technology that you use to access the internet are the property of OCA. Therefore, we reserve the right to monitor how you use the internet. We also reserve the right to find and read any data that you write, send, or receive through our online connections or that is stored in our computer systems.

The purpose of this Policy is to provide guidelines for the appropriate use of the internet by employees while on the organization's property or using organization-owned equipment. The internet is a valuable resource for conducting business and exchanging information, but it can also present security and liability risks. This Policy outlines the acceptable use of the internet and establishes consequences for violations.

Scope:

This Policy applies to all employees of the organization, including full-time, part-time, temporary, and seasonal employees, as well as contractors and consultants.

APPROPRIATE USE

The internet is intended to be used only for organization-related business purposes. Personal use of the internet is discouraged. However, limited personal use is permitted only if it does not interfere with job responsibilities or performance.

CONFIDENTIALITY

Employees are responsible for protecting confidential and proprietary information and must comply with all applicable laws and organization policies related to the protection of such information. Employees should not share confidential information or organization trade secrets on the internet.

ETHICAL CONDUCT

Employees must conduct themselves ethically and professionally while using the internet. Employees must not engage in any illegal or unethical activities, including, but not limited to:

- Harassment or discriminatory behavior
- Defamation or malicious gossip
- Infringement of intellectual property rights
- Downloading or distributing illegal or copyrighted material
- Conducting personal business or solicitations
- Accessing organization information that is not within the scope of one’s work
- Any form of gambling or pornography
- Playing of any games
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

UNACCEPTABLE USE OF INTERNET

- Sending or posting discriminatory, harassing, or threatening messages or images on the internet or via email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into websites
- Sending or posting information that is defamatory to the organization, its products/services, colleagues and/or customers
- Introducing malicious software onto the organization network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization.

SECURITY

Employees must take steps to protect the security of organization and customer information and must report any security incidents or violations to their supervisor or the Technology & IT Department.

MONITORING

The organization reserves the right to monitor employee internet use at any time to ensure compliance with this Policy.

CONSEQUENCES OF NON-COMPLIANCE

Violations of this Policy may result in disciplinary action, up to and including termination of employment. The organization may also take legal action against employees who engage in illegal activities on the internet. Internet access will be discontinued upon the termination of the employee or disciplinary action arising from violation of this Policy. In the case of a change in job function and/or transfer, the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

IT Asset Management Policy

Purpose:

The purpose of this IT Asset Management Policy is to ensure that all IT assets owned by OCA are identified, tracked, secured, and managed throughout their lifecycle in a consistent and standardized manner.

Scope:

This policy applies to all IT assets owned or leased by OCA, including but not limited to hardware, software, data, and network devices.

Policy:

1. Asset Identification and Inventory

   All IT assets owned or leased by OCA must be inventoried and identified. A unique identifier, such as a serial number or asset tag, should be assigned to each asset and recorded in the inventory.
2. Asset Tracking and Management

   All IT assets must be tracked throughout their lifecycle, including acquisition, deployment, maintenance, and disposal. Asset tracking should include information such as location, owner, maintenance records, and warranty information.
3. Asset Security

   All IT assets must be secured according to OCA's security policies and standards. Security measures may include physical security, network security, and access control.
4. Asset Disposal

   All IT assets must be disposed of in a secure and environmentally responsible manner. Assets should be securely wiped of all data and information before disposal. The disposal process should follow OCA's policies and guidelines for environmental sustainability.
5. Asset Procurement

All IT asset procurement must follow OCA's procurement policies and guidelines. The procurement process must include a review of the asset's impact on OCA's IT environment, including compatibility, security, and maintenance requirements.

6. Asset Maintenance and Upgrades
   All IT assets must be regularly maintained and upgraded as necessary to ensure they are functioning properly and meeting OCA's IT needs. Maintenance and upgrade schedules should be established and followed.
7. Asset Retention
   All IT assets should be retained for a specific period of time based on OCA's retention policies and guidelines. The retention period should be based on legal, regulatory, and business requirements.

Procedures

1. Asset Identification and Inventory
   - All IT assets must be inventoried and identified using a unique identifier such as a serial number or asset tag.
   - The inventory should include information such as asset type, manufacturer, model, and location.
   - The inventory should be updated regularly to ensure accuracy.

2. Asset Tracking and Management
   - All IT assets must be tracked throughout their lifecycle using an asset management system.
   - Asset tracking should include information such as location, owner, maintenance records, and warranty information.
   - The asset management system should be updated regularly to ensure accuracy.

3. Asset Security
   - All IT assets must be secured according to OCA's security policies and standards.
   - Security measures may include physical security, network security, and access control.

- Security controls must be regularly reviewed and updated to ensure effectiveness.

4. Asset Disposal
    - All IT assets must be disposed of in a secure and environmentally responsible manner.
    - The disposal process should follow OCA's policies and guidelines for environmental sustainability.
    - All data and information should be securely wiped from the asset before disposal.

5. Asset Procurement
    - All IT asset procurement must follow OCA's procurement policies and guidelines.
    - The procurement process must include a review of the asset's impact on OCA's IT environment, including compatibility, security, and maintenance requirements.
    - Procurement decisions must be documented and approved by authorized personnel

6. Asset Maintenance and Upgrades
    - All IT assets must be maintained according to the manufacturer's guidelines and OCA's maintenance policies.
    - The maintenance process should include regular check-ups, updates, and repairs as needed to ensure optimal performance.
    - Upgrades to IT assets should follow OCA's change management policies and guidelines.

7. Asset Retirement and Replacement
    - IT assets must be regularly assessed for their usefulness and relevance to OCA's IT environment.

- Outdated or no longer useful IT assets should be retired and replaced according to OCA’s retirement policies and guidelines.
- Replacement decisions must be documented and approved by authorized personnel.

Responsibilities

- OCA IT shall be responsible for managing the IT assets inventory, maintenance and disposal, including:
    - Maintaining accurate records of IT assets, including the asset type, location, owner, assigned user, warranty information, and purchase and disposal dates.
    - Developing and maintaining policies and procedures for IT asset management.
    - Ensuring that all IT assets are tracked and managed in accordance with these policies and procedures.
    - Conducting periodic audits to ensure compliance with these policies and procedures.
- Business unit managers shall be responsible for:
    - Ensuring that all IT assets assigned to their unit are properly managed and maintained.
    - Reporting all IT asset transfers, disposals, and purchases to OCA IT.
    - Verifying the accuracy of the IT assets inventory for their unit.
- End-users shall be responsible for:
    - Reporting any IT asset damage or malfunction to the IT helpdesk.
    - Reporting any lost or stolen IT assets to the IT helpdesk.
    - Complying with all IT asset management policies and procedures.

Asset Lifecycle Management

- Acquisition
    - 5.1.1 All IT asset acquisitions must be approved by the OCA Technology & IT department prior to purchase.
    - 5.1.2 OCA IT shall maintain a list of approved vendors for IT asset purchases.
    - 5.1.3 All IT asset purchases must be accompanied by a purchase order or approved requisition.
    - 5.1.4 All IT assets must be tagged with an OCA asset tag and entered into the IT asset inventory.

- Maintenance

  OCA IT shall be responsible for maintaining IT assets, including:

  - Installing and updating software and firmware as needed.
  - Performing preventive maintenance, including virus scans and hardware checks.
  - Performing repairs or arranging for repairs as needed.
  - Retiring or disposing of assets at the end of their useful life.

- Disposal
  - IT assets shall be disposed of in accordance with OCA IT's policies and procedures.
  - End-of-life IT assets must be securely erased or destroyed to prevent data breaches.
  - All IT assets must be removed from the IT asset inventory upon disposal.

Monitoring and Enforcement

- OCA IT shall periodically audit the IT asset inventory to ensure that all assets are properly tracked and accounted for.
- Any deviations from these policies and procedures shall be reported to the appropriate business unit manager and the OCA Technology & IT department.
- Any violations of these policies and procedures may result in disciplinary action, up to and including termination of employment.

Training

- All employees shall receive training on these policies and procedures as part of their onboarding process.
- Employees shall receive periodic refresher training on IT asset management policies and procedures.
- OCA IT shall provide training materials and resources for all employees to reference as needed.

Network Access Policy

Purpose:

The purpose of this policy is to define the rules and guidelines for granting network access to employees, contractors, vendors, and guests of the organization.

Scope:

This policy applies to all users who have access to the organization's computer network.

Policy:

- Access Control:
    - User Access: Network access will be granted to users who have a legitimate business need and have been authorized by their manager or supervisor.
    - Account Creation: Accounts for new employees will be created by the Technology & IT department after receiving authorization from the HR department. The Technology & IT department will ensure that accounts are created with appropriate levels of access.
    - Passwords: Passwords must be changed every 90 days, and must meet the minimum requirements for length, complexity, and expiration as specified by the Technology & IT department.
    - Authentication: Two-factor authentication will be required for remote access to the network.
- Network Security:
    - Firewall: The organization's network will be protected by a firewall that will filter incoming and outgoing traffic.
    - Antivirus: All computers connected to the network must have antivirus software installed and running. Antivirus software will be updated automatically.
    - Patch Management: All computers connected to the network must have the latest security patches installed. Patching will be done automatically.

  - Encryption: Sensitive data will be encrypted during transmission over the network.
  - Wireless Networks: Access to the organization's wireless network will be restricted to authorized users only. Wireless networks will be encrypted and have strong authentication.
- c. Monitoring and Auditing:
  - Logs: All network activity will be logged and monitored. Logs will be kept for a period of at least 6 months.
  - Auditing: The Technology & IT department will perform regular audits to ensure compliance with this policy.

Enforcement:

- Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.
- Any user who witnesses a violation of this policy must report it to their manager or supervisor.

Review and Revision:

- This policy will be reviewed annually by the Technology & IT department.
- Any changes to this policy must be approved by the Technology & IT department and communicated to all users.

Password Policy

Purpose:
The purpose of this policy is to establish guidelines for the creation, use, and management of strong passwords to protect OCA's information technology systems, network, and data from unauthorized access.

Scope:
This policy applies to all employees, contractors, and vendors who have access to OCA's information technology systems.

Policy:

- Password Creation:
  - Passwords must be a minimum of 12 characters in length and must contain a combination of uppercase and lowercase letters, numbers, and special characters.
  - Passwords must not contain easily guessable information, such as personal information, dictionary words, or common combinations.
  - Passwords must be unique and not used for any other system or service.
- Password Maintenance:
  - Passwords must be changed every 90 days.
  - Passwords must not be reused within a year.
  - Passwords must not be shared with anyone, including family members, colleagues, or supervisors.
  - Passwords must be entered privately and not left displayed on screens or written down.
- Password Security:
  - Passwords must be protected at all times and not left unattended or accessible to unauthorized persons.
  - Users must log out of their accounts when leaving their workstation or device unattended.
  - Accounts must be locked out after five unsuccessful attempts to log in.

  - Passwords must be encrypted during transmission and storage.
  - OCA reserves the right to perform periodic checks of passwords to ensure compliance with this policy.
- Password Reset:
  - Users who forget their passwords must contact the Technology & IT department to reset their password.
  - Users must verify their identity before a password reset can be performed.

Enforcement:

Any violation of this policy may result in disciplinary action, up to and including termination of employment, and legal action where appropriate.

Remote Access Policy

Purpose:

This policy provides guidelines for remote access to OCA's systems and data, ensuring secure and authorized access by remote employees, contractors, and third-party vendors. The policy applies to all OCA employees, contractors, and vendors who require remote access to OCA's systems and data.

Scope:

This policy applies to all employees, contractors, and vendors who require remote access to OCA's network and resources.

Policy:

- Access Authorization:
  Remote access to OCA's systems and data is strictly controlled and must be authorized by the Information Security Officer or their designated representative. All requests for remote access must be submitted in writing using the Remote Access Request Form and approved by the authorized personnel before access can be granted.
- Device and Software Requirements:
  All devices used for remote access to OCA's systems and data must meet the minimum-security requirements specified in the OCA's IT Security Policy. This includes up-to-date antivirus software, firewalls, and operating systems with the latest security patches and updates.
- Network Security:
  Remote access connections must use encryption technologies such as SSL or IPSec to ensure secure communication between the remote device and OCA's systems. All remote access connections must be routed through OCA's approved remote access gateway to ensure that only authorized users gain access to OCA's systems.
- Authentication:
  All remote access users must use secure and strong passwords to authenticate their identity. Two-factor authentication may be required for certain systems and applications based on the sensitivity of the data accessed.

- User Responsibilities:
  Remote access users must follow all OCA's IT Security policies and procedures, including protecting their remote access credentials from unauthorized access, reporting any security incidents or breaches immediately, and not sharing their remote access credentials with others.
- Termination of Access:
  Remote access privileges will be terminated immediately upon termination of the employee or contractor's employment, contract or agreement with OCA, or if the user's access is no longer required.
- Compliance Monitoring:
  OCA reserves the right to monitor remote access connections to ensure compliance with this policy and OCA's IT Security policies and procedures. All remote access users must agree to such monitoring as a condition of remote access.

Enforcement:

Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as legal action in case of unauthorized access or data breaches.

Security Response Plan Policy

Overview:

A Security Response Plan (SRP) is designed to coordinate security and operational teams in their crisis response (detection or exploitation of security vulnerability) and to integrate their efforts in terms of awareness and communication.

By requiring business units to incorporate an SRP as part of their business continuity activities and as new products or services are developed and prepared for marketing to consumers, they ensure that, when an incident occurs, prompt mitigation and correction measures are taken.

Purpose:

The purpose of this policy is to establish requirements for the development and maintenance of a security response plan for all business units supported by Information Security Team employees. This policy is also intended to provide the Security Incident Management Team with all the information necessary to formulate an effective response to a specific security incident.

Applicability:

This policy applies to all business units or entities within OCA.

Policy:

The development, implementation and execution of a Security Response Plan (SRP) is the responsibility of the business unit for which the SRP is being developed in collaboration with the Information Security Team.

OCA expects business units to adequately facilitate the SRP for the service or products for which they are responsible.

The Business Unit Security Coordinator must also work with the Information Security Organizational Unit to develop and update a Security Response Plan.

Service or Product Description:

The product description in an SRP must clearly define the service or application to be deployed with particular attention to data flows, logic diagrams and architecture.

Contact Information:

The SRP must include contact information for team members who will be available outside of business hours if a technological incident occurs and an escalation is required.

The SRP document must include all telephone numbers and e-mail addresses of the specialized team members. This may be a 24/7 requirement, depending on the defined business value of the service or product, combined with the impact on the customer.

Triage:

In order to quickly mitigate security vulnerability, the SRP should define the triage steps to be coordinated with the security incident management team in a cooperative manner. This step generally includes the validation of the reported vulnerability or compromise.

Identified Mitigations and Testing:

The SRP must include a defined process to identify and test mitigation measures before deployment. These details should include both short-term mitigation measures and the remediation process.

Mitigation and Remediation Timelines:

The SRP must include appropriate levels of response to identified vulnerabilities. It must define the expected repair times according to the seriousness and impact on the consumer, the brand and the organization. These intervention guidelines should be

carefully mapped according to the severity level, which should be determined according to the reported vulnerability.

Policy Compliance

Compliance Measurement:

Each business unit must have a written SRP, and this must be known to the employees concerned. The policy should be reviewed annually.

Non-Compliance:

Any business unit that has violated this policy may be sanctioned until an SRP is developed and approved.

In addition, those responsible may be subject to disciplinary action, up to and including termination, if a security incident occurs in the absence of an SRP.

Service Level Agreement (SLA) Policy

Purpose:

The purpose of this SLA is to define the level of services to be provided by the Help Desk to end-users and to establish the responsibilities of both parties.

Scope:

This SLA applies to all IT services provided by the Help Desk to end-users.
The Help Desk is responsible for providing Level 1 and Level 2 support to OCA's end-users. The services to be provided by the Help Desk include:

Incident Management - The Help Desk will provide incident management services to OCA's end-users. This includes logging, tracking, and resolving incidents related to hardware, software, and network issues.

Request Fulfilment - The Help Desk will provide request fulfilment services to OCA's end-users. This includes fulfilling requests for access to IT systems, software installation, and other IT-related requests.

Problem Management - The Help Desk will provide problem management services to OCA's end-users. This includes identifying the root cause of problems and implementing solutions to prevent their recurrence.

Change Management - The Help Desk will provide change management services to OCA's end-users. This includes managing changes to IT systems and applications, ensuring that all changes are properly documented and tested, and minimizing the impact of changes on OCA's operations.

Roles and Responsibilities:

The Help Desk and OCA shall each have certain roles and responsibilities under this SLA. These roles and responsibilities are as follows:

Help Desk:

- Provide Level 1 and Level 2 support to OCA's end-users.
- Ensure that all incidents, requests, problems, and changes are logged and tracked in the Help Desk ticketing system.
- Respond to incidents, requests, problems, and changes in a timely manner, as defined in the SLA.
- Escalate incidents, requests, problems, and changes to Level 3 support as required.
- Provide regular reports to OCA on the performance of the Help Desk.

OCA end-users:

- Provide the necessary information to the Help Desk to assist in the resolution of incidents, requests, problems, and changes.
- Cooperate with the Help Desk in the resolution of incidents, requests, problems, and changes.
- Abide by the policies and procedures established by the Help Desk.
- Provide regular feedback to the Help Desk on the quality of services provided.

Service Level Targets:

The Help Desk shall meet the following service level targets:

Incident Management:

- Severity 1 incidents (system down): The Help Desk shall respond within 30 minutes and resolve within 4 hours.
- Severity 2 incidents (major impact): The Help Desk shall respond within 1 hour and resolve within 8 hours.
- Severity 3 incidents (minor impact): The Help Desk shall respond within 4 hours and resolve within 24 hours.
- Severity 4 incidents (minimal impact): The Help Desk shall respond within 24 hours and resolve within 72 hours.

Request Fulfilment:

- Requests for access to IT systems: The Help Desk shall respond within 4 hours and fulfil within 24 hours.
- Requests for software installation: The Help Desk shall respond within 4 hours and fulfil within 48 hours.
- Other IT-related requests: The Help Desk shall respond within 4 hours and fulfil within 72 hours.

Problem Management:

- Problem identification and analysis: The Help Desk shall complete within 48 hours.
- Root cause analysis and resolution: Once the root cause of a problem has been identified, the Help Desk will work with the appropriate team(s) to determine a solution and timeline for resolution. The Help Desk will provide regular updates to the user until the problem has been resolved.
- Escalation: If a problem cannot be resolved within the time frame specified in the SLA, it shall be escalated to the appropriate level of management. The escalation process is as follows:

  Level 1: Help Desk staff
  The help desk staff is the first point of contact for end-users who need assistance. They are responsible for triaging tickets and determining the appropriate level of support. If the help desk staff can resolve the issue, they will do so. If the issue cannot be resolved, they will escalate the ticket to the next level of support.

  Level 2: Technical Support staff
  The technical support staff is responsible for resolving issues that are beyond the scope of the help desk staff. They may have access to more specialized tools and resources, and they may have more experience in resolving complex issues.

Level 3: External Vendors

In some cases, the issue may be so complex or specialized that it requires the assistance of an external vendor. In these cases, the technical support staff will work with the vendor to resolve the issue.

- Trend analysis and proactive problem management: The Help Desk will perform trend analysis on all problems and work with other IT teams to develop proactive measures to prevent future problems.
- Problem closure: The Help Desk shall notify the user when the problem has been resolved and shall ensure that the problem ticket is closed in a timely manner.

Change Management:

- Request for Change (RFC): Any changes to the IT infrastructure, applications or systems must be submitted via an RFC. The Help Desk shall log and prioritize all RFCs.
- Change assessment: The change management team shall review all RFCs to assess the impact of the change on the IT infrastructure, applications or systems.
- Change approval: RFCs shall be approved or rejected based on the impact assessment.
- Change implementation: Approved changes shall be implemented in accordance with the change management process.
- Post-implementation review: The change management team shall review the success of the change and ensure that any issues are addressed.

Performance Metrics:

- Help Desk availability: The Help Desk shall be available 8/5/365.
- Average speed to answer: The Help Desk shall answer calls within 5 seconds on average.
- First call resolution rate: The Help Desk shall aim to resolve 70% of calls on the first call.

- End Users satisfaction: The Help Desk shall measure end-users' satisfaction using surveys, with a target score of 9 out of 10.

Reporting:

- Monthly report: The Help Desk shall provide a monthly report to the Technology and IT Manager, which includes:
    - Number of calls received
    - Number of calls resolved
    - Average speed to answer
    - First call resolution rate
    - End Users satisfaction score

Review and Improvement:

- Review: The SLA shall be reviewed annually by the Technology and IT Manager and the Help Desk team.
- Improvement: Any issues or areas for improvement identified during the review shall be addressed in a timely manner.

Incident Policy

Purpose:

The Incident Response Policy and Procedures aim to establish guidelines for OCA employees in responding to security incidents that may affect the confidentiality, integrity, and availability of the organization's information and IT assets. This policy outlines the steps to be taken in the event of a security incident, the roles and responsibilities of the incident response team, and the reporting and communication procedures.

Scope:

This policy applies to all OCA employees who handle, process, or have access to the organization's information and IT assets.

Incident Response Team

An Incident Response Team (IRT) will be established to manage security incidents. The IRT will consist of the following members:

- Incident Response Coordinator: Responsible for coordinating the response to security incidents and overseeing the incident response process.
- IT Security Manager: Responsible for managing IT security, including incident response.
- IT Infrastructure Manager: Responsible for managing IT infrastructure, including the network, servers, and workstations.
- Legal Counsel: Responsible for providing legal advice on incident response matters.
- Public Relations Officer: Responsible for managing communication with external stakeholders, including the media and regulatory authorities.

Incident Response Procedures

The incident response procedures consist of the following steps:

- Identification and Reporting Any OCA employee who becomes aware of a security incident must report it immediately to the Incident Response Coordinator.

- Assessment and Classification Upon receiving an incident report, the Incident Response Coordinator will assess the incident to determine its severity and impact. The incident will be classified based on the following categories:
    - Low severity: Incidents that have a minimal impact on the organization's operations or information assets.
    - Moderate severity: Incidents that have a significant impact on the organization's operations or information assets.
    - High severity: Incidents that have a severe impact on the organization's operations or information assets, including data breaches and cyber-attacks.

Response and Containment

The IRT will develop a response and containment plan based on the incident classification. The plan will include the following actions:

- Isolation of affected systems and assets.
- Collection of evidence for forensic analysis.
- Mitigation of the incident to prevent further damage.
- Restoration of affected systems and assets.

Investigation and Analysis

The IRT will investigate the incident to determine the cause and origin. The investigation will include the following activities:

- Forensic analysis of affected systems and assets.
- Analysis of log files and system events.
- Interviewing witnesses and other relevant parties.
- Coordinating with law enforcement agencies, if necessary.

Notification and Communication

The IRT will notify and communicate with relevant stakeholders, including:

- Senior management: To provide updates on the incident and its impact.
- Partners: To inform them of the incident and its potential impact on their operations.
- Regulatory authorities: To comply with legal and regulatory requirements.

- Law enforcement agencies: To report incidents that may involve criminal activities.

Remediation and Follow-up

The IRT will develop a remediation plan to address the root cause of the incident and prevent its recurrence. The plan will include the following actions:

- Updating policies, procedures, and controls to prevent similar incidents.
- Training employees on incident response and security awareness.
- Conducting periodic reviews and audits to ensure compliance with the incident response policy.

Software Licensing Policy

Purpose:

The purpose of this policy is to ensure that all software used within OCA is properly licensed and in compliance with copyright laws, vendor agreements, and industry best practices.

Scope:

This policy applies to all OCA employees, contractors, and third-party vendors who use software as part of their job responsibilities or have access to OCA-owned devices and networks.

Policy:

OCA is committed to using only licensed software on all company-owned devices and systems. All employees and contractors are responsible for complying with all software licensing agreements and copyright laws. Failure to comply with this policy may result in disciplinary action, up to and including termination.

Licensing Procedure

All software used within OCA must be properly licensed. The Technology & IT department is responsible for managing software licensing and ensuring compliance with this policy. The following procedures must be followed:

- Software procurement:

  All software procurement must be approved by the Technology & IT department. Procurement of any software without prior approval is strictly prohibited.

- License tracking:

  The Technology & IT department is responsible for tracking all software licenses, including the number of licenses purchased, their expiration dates, and any renewals or upgrades.

- License compliance:

  All software must be used in compliance with the licensing agreement. If any software is used in violation of the license agreement, it must be immediately reported to the Technology & IT department.

- Software removal:

  All software must be removed from company-owned devices and systems when no longer in use or when the license has expired.

Employee Responsibility

All employees are responsible for complying with this policy and ensuring that the software they use is properly licensed. Specifically, employees must:

- Use software only in accordance with its license agreement.
- Report any unlicensed software immediately to the Technology & IT department.
- Not install software on any OCA-owned device without prior approval from the Technology & IT department.
- Remove any software that is no longer in use or has expired.

Consequences of Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination. In addition, any employee found to have violated copyright laws or software licensing agreements may be subject to legal action and financial penalties.

System Maintenance Policy

Purpose:

The purpose of this policy is to ensure that all OCA systems are properly maintained to ensure their availability, reliability, and security.

Scope:

This policy applies to all OCA employees, contractors, and third-party vendors who are responsible for maintaining OCA systems.

Policy:

- Regular Maintenance
  All OCA systems must undergo regular maintenance to ensure their proper functioning. This includes regular software updates, security patches, backups, and other necessary maintenance activities.
- Scheduled Maintenance
  Windows All maintenance activities that may impact system availability must be scheduled during pre-approved maintenance windows. These windows will be communicated in advance to all affected parties.
- Emergency Maintenance
  In case of an emergency maintenance situation, OCA IT staff will immediately work to resolve the issue. In such cases, they will notify all affected parties as soon as possible.
- Change Management
  All changes to OCA systems, including software updates and hardware modifications, must be approved through the OCA change management process. This process ensures that any potential risks are identified and mitigated prior to implementation.
- Testing and Validation
  All changes made to OCA systems must be thoroughly tested and validated prior to implementation to ensure that they do not cause any unexpected problems.

- System Availability
  OCA systems must be available at all times during normal business hours. In the event of scheduled maintenance or unexpected downtime, IT staff will work to restore system availability as soon as possible.
- System Monitoring
  All OCA systems must be continuously monitored for performance issues and potential security breaches. IT staff will take proactive measures to address any issues that arise.

Responsibilities

- IT Staff
  OCA IT staff are responsible for maintaining all OCA systems in accordance with this policy.
- Employees
  All OCA employees are responsible for reporting any system issues or potential security breaches to the Technology & IT department.
- Contractors and Third-Party
  Vendors All contractors and third-party vendors who perform system maintenance activities on behalf of OCA must adhere to this policy.

Technology Policy

Intent:

The primary intent of this Policy is to increase protection of Technology Resources to assure the usability and availability of those resources to all users at OCA (the "Organization"). The Policy also addresses privacy and usage guidelines for those who access the Organization's Technology Resources.

Scope:

The Organization recognizes the vital role technology plays in effecting Organization business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by authorized users, the need for an increased effort to protect the information and the Technology Resources that support it, is felt by the Organization, and hence this Policy. Since a limited amount of personal use of these facilities is permitted by the Organization for users, including computers, printers, email, software and Internet access, therefore, it is essential that these facilities are used responsibly by users, as any abuse has the potential to disrupt Organization business and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using the Organization's technology facilities.

Definition:

- Information Technology. Information Technology Resources for the purposes of this Policy include but are not limited to the Organization's owned or those used under license or contract, or those devices not owned by the Organization but intentionally connected to the Organization's owned Technology Resources such as computer hardware, printers, fax machines, voicemail, software, email and Internet and intranet access.

- User. Anyone who has access to Organization's Technology Resources, including but not limited to, all employees, temporary employees, probationers, contractors, vendors, and suppliers.

Access Control:

Access control is a crucial part of ensuring the security and confidentiality of OCA's technology and IT systems. It is the responsibility of the Technology and IT Department to manage access to OCA's technology resources and to ensure that the access control policy is followed by all employees.

Access Rights and Permissions

Access rights and permissions to OCA's technology resources will be granted only to authorized personnel who have a legitimate need to access them. Access will be granted on a need-to-know basis and will be based on the employee's job duties and responsibilities.

User Identification and Authentication

All users will be required to identify themselves by providing a unique username and password to access OCA's technology resources. Strong passwords that meet the OCA's password policy guidelines must be used. Employees are responsible for keeping their passwords confidential and should not share them with anyone.

Password Management

The Technology and IT Department will enforce a password policy to ensure that all passwords are strong and difficult to guess. Passwords will be changed periodically, and employees will be required to use a combination of letters, numbers, and special characters to create a strong password.

Access Monitoring and Review

The Technology and IT Department will monitor access to OCA's technology resources and periodically review access logs to ensure that access is granted only to authorized personnel. Access logs will be reviewed to identify any unauthorized access attempts or suspicious activity.

Termination of Access

When an employee leaves the organization or changes job roles, their access to OCA’s technology resources will be terminated or adjusted according to their new job duties. The Technology and IT Department will ensure that access is promptly removed or modified.

Physical Access Control

Physical access control refers to the measures taken to control who can access the physical premises of the OCA Technology and IT Department. All employees, contractors, and visitors must follow these measures to ensure the security of the department's physical assets and data.

a. Access Authorization

Access to the OCA Technology and IT Department's physical premises is authorized based on job responsibilities and need-to-know. Access requests must be approved by the appropriate department head, and all personnel must follow the access control procedures outlined in this policy.

b. Key and Access Card Control

Access keys and cards must be kept secure and not be shared with unauthorized individuals. Employees must return their keys and access cards when they leave the OCA Technology and IT Department, or when their employment ends.

c. Visitor Access Control

All visitors must be escorted while in the OCA Technology and IT Department's physical premises and must be issued temporary access badges or passes. Visitors must be registered and authorized by a department head or supervisor prior to arrival.

Remote Access Control

Remote access to OCA’s technology resources will be granted only to authorized personnel who have a legitimate need to access them. Remote access will be granted on a need-to-know basis and will be based on the employee’s job duties and responsibilities.

Mobile Device Management

Mobile devices, such as smartphones and tablets, that access OCA's technology resources will be managed to ensure that they meet the OCA's security standards. Mobile devices that are lost or stolen will be remotely wiped to prevent unauthorized access to OCA's technology resources.

Reporting Security Incidents

Employees are required to report any security incidents or suspicious activities immediately to the Technology and IT Department. The Technology and IT Department will investigate all reported security incidents and take appropriate actions to mitigate any potential security risks.

Network Access Control

Network access control refers to the measures taken to control who can access the OCA Technology and IT Department's network and data. All employees, contractors, and visitors must follow these measures to ensure the security of the department's network and data.

a. Access Authorization

Access to the OCA Technology and IT Department's network and data is authorized based on job responsibilities and need-to-know. Access requests must be approved by the appropriate department head, and all personnel must follow the access control procedures outlined in this policy.

b. User Accounts and Passwords

All user accounts must be created and managed by the IT department, and passwords must be changed on a regular basis. Passwords must meet minimum complexity requirements and must not be shared with unauthorized individuals.

c. Remote Access Control

Remote access to the OCA Technology and IT Department's network and data is only allowed through authorized channels and must be secured using multi-factor authentication.

MANAGING SYSTEM PRIVILEGES

Requests for new user-IDs and changes in privileges must be made to the IT Department by email. Users must clearly state why the changes in privileges are necessary.

In response to feedback from the Human Resources Department, the IT Department will revoke any privileges no longer needed by users. After receiving information from the HR Department, all system access privileges will be terminated within 24 hours when a user leaves the Organization. The Organization's management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of the Organization's information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

SECURITY (ACCESS CONTROL)

Users are forbidden from circumventing security measures. Users are strictly prohibited from establishing dial-up connections, using modems or other such apparatus, from within any Organization premises. Users who have been given a mobile/portable laptop or any other device and duly authorized for such remote access, which connects to the Organization's mail system on a real-time basis, can do so through the Internet.

Unless the prior approval of the Technology and IT Manager has been obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to the Organization's systems and information. These connections include the establishment of multi-computer file systems, Internet web pages and FTP servers. Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in

writing by the Technology and IT Manager. Incidents involving unapproved system cracking or hacking, password cracking, file decryption, software copying, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of the Organization's Policy. Likewise, short-cuts bypassing system security measures are absolutely prohibited.

CHANGES TO SYSTEMS

No user must physically connect or disconnect any equipment, including Organization-owned computers and printers, to or from any Organization network. Except for emergency situations, all changes to the Organization's technology systems and networks must be documented and approved in advance by the Technology and IT Manager. Only persons who have been authorized by the Technology and IT Manager can make emergency changes to any Organization computer system or network.

Third-Party Access Policy

Purpose:

The purpose of this policy is to establish guidelines for granting and managing third-party access to OCA systems, networks, data, and resources. This policy aims to ensure that third-party access is granted only when necessary and is conducted in a secure and controlled manner, minimizing the risk of unauthorized access or misuse of OCA information.

Scope:

This policy applies to all third-party vendors, contractors, consultants, and other non-employee individuals who require access to OCA systems, networks, data, and resources.

Policy:

Approval Process:

- All requests for third-party access must be approved by OCA management before access is granted.
- The request must include the purpose of the access, the type of access required, the duration of the access, and the identity of the third-party requiring access.
- The approval must be granted in writing and documented in the third-party access request.

Types of Access

- Remote Access
  - All remote third-party access must be through a secure VPN connection.
  - All remote access must require a unique username and strong password.
  - Access must be terminated immediately after the authorized purpose of the access has been completed.

- Physical Access
  - Third-party access to OCA facilities must be limited to areas necessary to perform the authorized work.
  - Physical access must be granted only during authorized times and monitored by OCA staff.
  - Third-party personnel must be escorted by OCA personnel when accessing OCA facilities.

Data Access

- Third-party access to OCA data must be limited to the data necessary to perform the authorized work.
- Access to sensitive or confidential information must be granted only on a need-to-know basis.
- Access must be terminated immediately after the authorized purpose of the access has been completed.

Security Requirements

- All third-party access must comply with OCA's information security policies and procedures.
- All third-party personnel must undergo a background check and sign a confidentiality agreement.
- Third-party personnel must comply with OCA's security awareness training requirements.
- OCA must monitor all third-party access to its systems, networks, and data.

Termination of Access

- Third-party access must be terminated immediately upon the completion of the authorized work.
- Third-party access must be terminated immediately upon the termination of the third-party's contract with OCA or upon termination for any other reason.
- Access must be terminated immediately upon discovery of unauthorized access, security breaches, or policy violations.

Compliance Monitoring

- Compliance with this policy must be reviewed on a regular basis by the OCA Technology & IT department.
- OCA must conduct periodic reviews of third-party access to ensure compliance with this policy.
- Any violations of this policy must be reported immediately to the appropriate OCA management and the Technology & IT department.

Virtual Private Network (VPN) Policy

Purpose:

The purpose of this policy is to provide guidelines for the appropriate use of Virtual Private Network (VPN) technology to ensure the confidentiality, integrity, and availability of OCA's data and resources.

Scope:

This policy applies to all employees, contractors, consultants, and third-party service providers who require access to OCA's network resources through the use of VPN.

Policy:

VPN Access

- Access to OCA's network through VPN must be approved by authorized personnel.
- Only authorized users with a valid business need should be granted VPN access.
- VPN access must be restricted to the minimum necessary privileges required to complete the task at hand.
- Users must log out of VPN sessions when they are no longer needed.

VPN Client Software

- Only authorized VPN client software may be used to connect to OCA's network.
- VPN client software must be installed and configured by authorized personnel.
- Users must ensure that VPN client software is kept up-to-date with the latest security patches and updates.
- VPN client software must not be installed on unapproved devices.

Encryption

- All VPN traffic must be encrypted using strong encryption algorithms.

- Encryption keys must be managed securely and changed periodically.
- Users must not share their VPN credentials with others.
- All VPN sessions must be terminated if a user's credentials are suspected of being compromised.

Authentication

- VPN users must be authenticated using strong authentication methods, such as two-factor authentication.
- Passwords for VPN access must meet OCA's password policy requirements.
- VPN accounts must be disabled or deleted when a user no longer requires VPN access.

Procedures:

VPN Access Request

- Users who require VPN access must complete a VPN Access Request Form.
- VPN Access Request Forms must be approved by authorized personnel before access is granted.
- Approved VPN Access Request Forms must be kept on file.

VPN Client Installation and Configuration

- VPN client software must be installed and configured by authorized personnel.
- Users must not attempt to install or configure VPN client software on their own.

VPN Session Management

- Users must log out of VPN sessions when they are no longer needed.
- Authorized personnel must monitor VPN sessions for unusual activity.
- VPN sessions must be terminated immediately if suspicious activity is detected.

VPN Disconnection

- VPN sessions will be disconnected after a period of inactivity in accordance with OCA's security policy.
- Users must save their work and log out of VPN sessions before the disconnection timer expires.

VPN Access Review

- Authorized personnel must review VPN access privileges regularly.
- VPN access privileges must be revoked when a user no longer requires VPN access.

Wireless Network Policy

Purpose:

The purpose of this policy is to establish guidelines for the secure use and management of wireless networks within OCA. This policy applies to all employees, contractors, and third-party vendors who use wireless networks to access OCA's network and systems.

Scope:

This policy applies to all wireless network devices, including but not limited to access points, routers, switches, and other wireless-enabled devices used to connect to OCA's network.

Policy:

Wireless network security:

- All wireless networks used by OCA must use WPA2 or WPA3 encryption protocols to ensure the confidentiality of the information transmitted over the network.
- Wireless networks must be secured with a unique, strong password that is changed regularly.
- Wireless networks must be regularly scanned for vulnerabilities, and any detected vulnerabilities must be remediated in a timely manner.
- Only authorized personnel with a legitimate business need should be allowed access to wireless networks.
- All wireless access points and devices must be installed and configured by authorized personnel only.

Guest wireless access:

- Guest wireless access must be isolated from the main network and should be assigned to a separate VLAN or subnet.
- Guest wireless access must be secured with a password that is changed frequently.

- Guest wireless access must be provided only to authorized individuals, and guests should be required to sign an agreement acknowledging their acceptance of the terms and conditions of the guest wireless access.

Wireless network usage:

- Wireless networks must be used only for business purposes.
- Wireless networks must not be used for personal purposes.
- Unauthorized devices must not be connected to the wireless network.
- OCA reserves the right to monitor wireless network usage to ensure compliance with this policy and other applicable policies.

Procedures:

Wireless network device management:

- All wireless devices must be registered with OCA's Technology & IT department before they can be connected to the network.
- All wireless network devices must be configured in accordance with OCA's wireless network security standards.
- Wireless network devices must be regularly scanned for vulnerabilities.

Guest wireless access:

- Requests for guest wireless access must be submitted to the Technology & IT department for approval.
- A unique password must be generated for each guest wireless access request, and the password must be changed after a predetermined period of time.
- Guests must be provided with an agreement to sign acknowledging their acceptance of the terms and conditions of the guest wireless access.

Wireless network usage:

- All users must be trained on the appropriate use of wireless networks and the risks associated with unauthorized usage.
- Users must comply with this policy and other applicable policies.
- Unauthorized usage must be reported to OCA's Technology & IT department immediately.

Software Development Life Cycle (SDLC) Policy

Purpose:

The purpose of this policy is to establish guidelines and standards for the System Development Life Cycle (SDLC) to ensure that all OCA projects are completed in a consistent, repeatable, and reliable manner.

Scope:

This policy applies to all OCA IT projects and systems that involve the development, enhancement, or maintenance of software applications or IT infrastructure. This policy is intended to provide guidance to project managers, developers, testers, business analysts, and other stakeholders involved in the SDLC.

Policy:

The purpose of this policy is to define the System Development Life Cycle (SDLC) methodology and procedures to be used by the Information Technology (IT) department of OCA in order to ensure that all software systems developed and maintained within the organization meet high standards of quality, reliability, security, and compatibility with existing IT infrastructure and business processes.

Procedures:

Planning Phase:

During this phase, the following procedures must be followed:

- Identify the scope of the project, its objectives, and business requirements.
- Identify the available resources (including personnel, hardware, and software) required for the project.
- Define the project timeline and milestones.
- Prepare a detailed project plan.
- Develop a project charter that outlines the project scope, objectives, assumptions, and constraints.

Analysis Phase:

During this phase, the following procedures must be followed:

- Analyze the requirements of the project stakeholders and end-users.
- Develop functional and technical specifications.
- Evaluate the feasibility of the project in terms of cost, resources, and timeline.
- Identify and evaluate any risks associated with the project.

Design Phase:

During this phase, the following procedures must be followed:

- Develop a detailed system design that meets the requirements of the stakeholders and end-users.
- Prepare detailed documentation, including technical specifications, design diagrams, and user manuals.
- Evaluate and select the appropriate hardware, software, and networking infrastructure to support the system.

Development Phase:

During this phase, the following procedures must be followed:

- Develop the software code according to the approved design specifications.
- Conduct unit testing to ensure that each module of the software functions correctly.
- Integrate the various modules of the software into a complete system.
- Conduct system testing to ensure that the software functions correctly as a whole.

Implementation Phase:

During this phase, the following procedures must be followed:

- Install the software on the production server or other designated hardware.
- Conduct user acceptance testing to ensure that the software meets the requirements of the stakeholders and end-users.
- Train end-users on how to use the software.
- Prepare the software for deployment to the production environment.

Maintenance Phase:

During this phase, the following procedures must be followed:

- Provide ongoing support and maintenance to the software.
- Conduct periodic audits and assessments of the software to ensure that it meets the needs of the stakeholders and end-users.
- Monitor the software for any issues or bugs and apply patches or updates as needed.
- Make enhancements or modifications to the software as requested by the stakeholders and end-users.

Decommissioning Phase:

During this phase, the following procedures must be followed:

- Determine when the software will no longer be needed.
- Develop a decommissioning plan that outlines how the software will be removed from the production environment.
- Conduct any necessary data migration or archiving activities.
- Remove the software from the production environment in a safe and secure manner

Project Management Policies and Procedures

Purpose:

The purpose of this document is to determine the exact project outcome for OCA. This plan also considers the degree of success of the project, including the methods of project measurement and communication. One of the most important reasons for the Project Management Plan is providing guidance when certain difficulties occur during the project.

As a project manager in OCA, it's imperative to examine the Project Management Plan to solve problems when they emerge. The document highlights specific issues that may occur and how to handle them for the best outcome.

Goals:

In the course of completing this document, the project manager will highlight the goals and priorities within your organization and develop a plan to achieve such goals. These goals can include any of the following:

- Successful development and implementation of necessary project procedures
- Achievement of a specific project's main goal within given constraints
- Productive guidance, accurate supervision, and effective communication

Objectives:

The primary objective of a Project Management Plan is to optimize allocated necessary inputs to achieve pre-defined objectives. Project managers can effectively work on reforming and upgrading project plan processes to enhance project sustainability. With the document, OCA may decide to reshape or reform the client's vision into feasible goals.

Roles and Responsibilities:

All activities and tasks defined in the project should fall within the scope of OCA's project. However, the project management process is the sole responsibility of the project manager. This individual is in charge of the project from start to finish. Here's a detailed breakdown of the roles and responsibilities of the project manager, project team member, project sponsor, executive sponsor, and business analyst.

Project Manager Responsibilities

The project manager's responsibilities are imperative for the success of the project. In most cases, OCA’s project manager’s duties aren't overly challenging or complex. Here's a breakdown of their responsibilities:

- Planning and developing of project idea
- Creating and leading a team
- Monitoring project progress and setting deadlines
- Evaluating project performance
- Resolving issues that arise
- Managing OCA's finances
- Ensuring stakeholder satisfaction

Project Team Member Responsibilities

In OCA, the project team members are responsible for actively working on one or more phases of the project. These individuals may be external consultants or in-house staff working on the project on a part-time or full-time basis. Here's a breakdown of the responsibilities of a project team member:

- Documenting the project process
- Providing expertise during project completion
- Contributing to the overall project goals and objectives
- Working with users to establish and meet required business needs

Project Sponsor Responsibilities

A project sponsor is the driver of the project. In most cases, the sponsor is typically a member of the senior management. Such individuals also have a stake in the project's outcome. In OCA, the project sponsor works closely with the project manager. These people also help remove obstacles that occur throughout the project lifecycle. Here are the significant responsibilities of a project sponsor:

- Making crucial business decisions for the project
- Ensuring adequacy and availability of resources
- Communicating project goals throughout OCA
- Approving project budget

Executive Sponsor Responsibilities

The executive sponsor at OCA is a high-ranking member of the management. As an important part of the management, such individuals are responsible for decision making and final approval. Here are the responsibilities of an executive sponsor:

- Providing additional funds for major changes
- Approving deliverables
- Approving changes to project scope
- Carrying final responsibility for the project

Business Analyst Responsibilities

OCA's business analyst is responsible for defining the business needs and recommending solutions for better organizational function. When participating on the team, the business analyst ensures project objectives solve the current business challenges.

This individual also ensures project objectives enhance performance and improve the organization's value. Here are the crucial responsibilities of the business analyst:

- Assisting in project definition
- Gathering requirements from users or business units
- Verifying project deliverables meet requirements
- Testing solutions to endorse project objectives
- Accurately documenting technical and business requirements

Project Management Plan

Once the responsibilities of employees and the management are clear, it becomes imperative to follow the appropriate Project Management Plan. Here's a breakdown of OCA's Project Management Plan:

Project Management Schedule

Here is OCA's summarized schedule for each phase and activity within the project lifecycle:

S/N	Task Name	Duration
1.	INITIATION	[NUMBER OF DAYS]
2.	PLANNING	[NUMBER OF DAYS]
3.	EXECUTION	[NUMBER OF DAYS]
4.	CLOSURE	[NUMBER OF DAYS]

Dependencies

OCA's dependencies are logical connections between phases, activities, or tasks that affect the entire project. Dependencies may be internal or external to the project. Here are the significant types of dependencies:

1. Finish to start *(The item this depends on must "finish" before it "starts")*
2. Start to finish *(The item this depends on must "start" before activity "finishes")*
3. Finish to finish *(The item this depends on must "finish" before activity "finishes")*
4. Start to start *(The item this depends on must "start" before it "starts")*

OCA's key project dependencies are identifiable from the table below:

Activity	Depends On	Dependency Type
Project Office	*Appoint Reliable Project*	*Finish to start*

	Team	

From the table above, it can be noted that it is imperative that "Appoint Reliable Project Team" should finish before "Set up the Project Office."

Assumptions

Here are some of OCA's planning assumptions:

- No change in the project scope
- Identified resources will be available upon request
- All approved funding will be available upon request

Constraints

Some planning constraints for OCA include:

- Project should operate within approved funding and resource allocations
- Project team should deliver the project with no requirement for extra funding
- Staff should complete the project within appropriate working hours

Action Plan

Following the creation of a detailed Project Management Plan, you need a viable action plan on how to implement the planning phases and the final plan.

Key Personnel

Assign the key personnel and the duties and responsibilities for project management. The list of assigned staff must be updated and distributed amongst the key people. The significant OCA key personnel include:

- Project manager
- Project team member

- Project sponsor
- Executive sponsor
- Business analyst

Milestones

OCA will follow a list of important milestones for the project, including the estimated time of completion. Some important milestones to determine include:

- Business Case approved
- Feasibility Study approved
- Project Charter approved
- Appointment of Project Team
- Establishment of Project Office

Here is a table to follow:

Milestone	Description	Delivery Date
Business Case Approved	The Project Sponsor documents and approves the Business Case	xx/yy/zz

Implementation

Month 1

Summarize the key tasks to be completed during the first month of the Project Management Plan.

Task/Procedure	Status	Responsible person

Subsequent Months

Explain the implementation of the Project Management Plan for the subsequent months, as needed. Focus on strategic tasks.

Task/Procedure	Status	Responsible person

General Services Policies and Procedures

Purpose:

The purpose of the General Services Policy is to provide guidelines and procedures for the efficient and effective management of general services within an organization. The policy aims to ensure that all employees have access to necessary resources and support services to carry out their work effectively. It outlines the organization's commitment to providing a safe, clean, and well-maintained work environment, as well as the procurement and management of equipment, supplies, and facilities.

Policy:

- General Services Policy:
  - Developing maintenance plans, programs, and arrangements for buildings, furniture, and equipment of OCA.
  - Taking actions to contract maintenance and cleaning services and monitoring their execution in coordination with the relevant administrative units.
  - Monitoring communication services and ensuring the payment of associated costs.
  - Supervising communication services, electricity, water, air conditioning, lighting, and other necessary services for the safety and efficiency of OCA's operations.
  - Developing security and safety plans and monitoring their implementation.
  - Supervising the employees of OCA, including workers, and distributing them among different administrative units according to work needs and requirements.
  - Identifying and providing OCA's procurement and service needs, and establishing the necessary specifications in coordination with the relevant administrative units, including them in the annual budget project of OCA.
  - Receiving and storing items in the proper manner, monitoring their movement, and meeting the needs of different administrative units. Supervising the warehouses and maintaining the necessary records in this regard.

- Taking the necessary measures to allocate government housing to OCA employees and providing furniture allowances to them in coordination with the relevant authorities.
- Handling all matters related to visas and residency permits for OCA employees from Kuwait.

Facility Management:

- The General Services team is responsible for ensuring that OCA's facilities and buildings are always clean and in good condition.
- The General Services team is responsible for maintaining office facilities and OCA's buildings, including:
  - Designing and implementing a preventive maintenance plan for office facilities.
  - Managing office assets, facility repairs, and replacement operations.
  - Ensuring the proper functioning of water supplies, plumbing services, sewage systems, and electrical power in OCA.
  - Supervising workers and carrying out minor civil works as necessary.
  - Maintaining air conditioning units, water coolers, refrigerators, and other electronic devices.
  - Ensuring the availability of maintenance tools, equipment, and supplies.
- The General Services Department may engage external resources to perform departmental responsibilities, including facility management, maintenance, and security. The General Services team continuously monitors the performance of third parties.
- The General Services team develops a maintenance plan in accordance with OCA's maintenance requirements.
- The General Services team records all maintenance activities to document and monitor the status of these activities and provides reports to relevant parties to facilitate decision-making.
- The General Services Department maintains a list of vendors and price lists for all external contractors, such as elevator maintenance, cleaning services, website design, and security equipment.
- When utilizing external resources for maintenance work, the General Services Department considers applicable warranties.

- The General Services team is responsible for ensuring energy efficiency in OCA's office buildings and monitoring the implementation of energy conservation programs.
- All maintenance work in offices should be carried out after the designated working hours, except in emergency cases. The General Services team promptly responds to emergency requests.

Office Privileges:

- Office Space:
  - The plan related to office space and its size is prepared by the General Services team.
  - Offices and workspace are distributed to employees based on job level, nature of work, and availability of offices.
- Parking Spaces:
  - Prior approval from the General Services Manager is required for all requests related to parking services for OCA employees, and priority is determined based on job level, nature of work, and availability of parking spaces.
  - The General Services Department is responsible for controlling and monitoring access to parking spaces.
- Signage/Advertising Boards:
  - The General Services team ensures the presence of signage and advertising boards in OCA buildings, in coordination with the Public Relations and Communications Department, to reflect the image and identity of OCA.
- Stationery and Office Supplies:
  - The General Services Department is responsible for providing employees with the daily-used office supplies, and the General Services Department is responsible for distributing and maintaining the office supplies in OCA
  - departments. Office supplies are organized in cabinets, shelves, or file cabinets.
  - Issuing/providing expensive/non-essential items, such as computer docking stations or additional computer screens, requires approval from the relevant department managers and the General Services Manager.

- Communication Supplies:
  - OCA maintains a substantial stock of previously printed papers obtained from the General Services team.
- Printers, Copiers, and Shredders:
  - All preparations for installing printers, copiers, and shredders are done in dedicated rooms, and workspace is arranged to accommodate the equipment.
  - When the work requires the installation of other large specialized equipment/machines, the appropriate and secure space must be determined and allocated.
  - All employees are prohibited from using office spaces, equipment, supplies, stationery, and publications for personal reasons.

Health and Safety:

- Management of Employees/Visitors
  - The General Services team should provide appropriate security services to maintain public safety and control access to OCA facilities and offices.
  - The department is responsible for ensuring that only authorized visitors enter the workplace, helping prevent unauthorized visitors from compromising safety standards, protecting against theft, ensuring equipment protection, safeguarding confidential information, protecting employee interests, and avoiding distractions and disruptions.
  - Access should only be granted to individuals who possess identification documents or permits.
  - Security guards are responsible for monitoring the entry and exit of employees and visitors and controlling the entry and exit of materials and goods.
  - Authorized visitors should receive instructions or be accompanied by reception staff to their destinations, and the employees are responsible for the behavior and safety of their visitors.
  - If an unauthorized person is noticed in OCA buildings, employees should direct this person immediately to the security gate and reception.

- Security guards should open and maintain records to record the entry and exit of visitors to OCA buildings, and security guards should keep records of the entry and exit of employees and workers outside of working hours.

- OCA Security Management
  - Employees are responsible for protecting OCA office supplies, including all equipment and assets at all times.
  - The General Services Department should investigate theft, loss, or damage cases involving OCA property and should contact local police, security, and other government institutions as necessary.
  - The Facilities Management department is responsible for managing the issuance of keys/access cards for OCA employees and should maintain an updated record for this purpose.
  - Security guards should be familiar with different locations, departments, access routes, and access rights.
  - Security guards should conduct patrols in designated areas, including parking lots and public/common areas, and check for suspicious incidents.
- Safety and Fire Management
  - The General Services Department is responsible for the design, installation, update, inspection, maintenance, and testing of all fire safety equipment, including fire extinguishers, smoke detectors, alarm systems, first aid kits, etc.
  - Periodic inspections should be conducted on fire exits, security control panels, fire alarm systems, and related security equipment.
  - The General Services Department should prepare a "Fire and Safety Report" every 3 months after inspection and maintenance to assess the condition of safety equipment, deviations, and exceptions.
- Security Management
  - For any external meetings or events, security checks should be conducted at those locations, and based on that, the General Services Department should organize appropriate security for these events.
  - The General Services Department monitors all public areas in OCA, reports all violations, and escalates them accordingly.
  - All areas with high-security risks should be equipped with intrusion alarms.

- All security alarm systems should be monitored and connected to a predefined response system.
- The General Services team should appoint individuals responsible for firefighting and first aid provision and provide necessary training for them.
- Firefighting and first aid responsible individuals should be assigned in designated OCA locations, and their contact details should be made available to all employees.

Reception:

- Every receptionist should be polite, act professionally, have a neat and appropriate appearance, and care for the clients and visitors of the organization.
- Receptionists should choose appropriate concise words when answering phone calls.
- The General Services Department is responsible for monitoring receptionists and their behavior at all times.
- Receptionists should be aware of the reason for the visit of non-employee individuals to the organization/visitors who wish to enter the organization's offices, and they should inform the relevant employee about this visit.
- Visitors are not allowed to enter or exit the reception area without receiving prior instructions from the designated employee unless accompanied by a security guard.
- For security reasons, visits by the families or friends of employees are not permitted. In emergency situations, contacting the employee to meet their visitor outside working hours is required.

Meeting Rooms and International Calls

- Meeting Rooms
  - Meetings are scheduled by the General Services team.
  - Requests for scheduling meeting rooms can be made via email, in person, or through telephone calls.
- International Calls
  - As per the organization's policy, certain employees are designated to use international call lines, based on their job requirements and role.

- To maintain a fair and appropriate policy in facilitating access to telephone calls made by employees, the General Services Department, in coordination with the Technology and Information Department, ensures that password activation is implemented on each communication device for monitoring and tracking purposes.
- Personal international calls are not allowed for employees. In case of an emergency requiring an international call, the employee should inform the General Services Department.

Transportation Management:

- The department is responsible for managing the rented and owned vehicles used to meet the needs and purposes of the organization's work. For this purpose, the department maintains an updated record of all vehicles in the organization, including:
  - Vehicle details and information (vehicle type, service start date, registration plate number, etc.).
  - Maintenance history/schedule (for owned vehicles).
  - Insurance details and information for owned vehicles (insurance type, coverage period, renewal dates, etc.).
  - Vehicle ownership (rented or owned).
- The use of organization vehicles is allowed during official working hours and approved tasks outside working hours.
- The department is responsible for renting vehicles to meet the organization's needs in coordination with the procurement team. It is essential to ensure that all rented vehicles are fully insured by the third party/rental company.
- The department determines the authorized drivers/employees to use organization vehicles and ensures that they hold a valid driver's license when using the vehicles. The department maintains a record of authorized vehicle users, indicating their personal information, contact numbers, and driver's license expiration dates.
- The department keeps a daily log of vehicle usage, including at least:
  - Driver/employee information.
  - Vehicle details.
  - Purpose of vehicle usage.
  - Time of vehicle pick-up.

    - Time of vehicle return.
- The employee/driver is responsible for the proper use of the vehicle, refueling as needed (using vouchers/agreements with fuel stations), and reporting any malfunctions or issues to the General Services Department.
- The department conducts regular monitoring to check for any violations or fines to avoid accumulation. Coordination with the Human Resources Department and the concerned employee/driver is done to address any violations issued against organization vehicles.
- The department is responsible for liaising with relevant authorities in the event of accidents, including car rental agencies, traffic departments, insurance companies, and others.

Delivery of Assets to Organization's Warehouses:

- The General Services Department is responsible for ensuring the safe transportation of assets to and from the organization's buildings. For this purpose, the organization can appoint logistics service providers capable of executing the asset transportation process.
- All assets being delivered to the organization's buildings are securely loaded onto equipped vehicles, with qualified drivers and workers, to ensure the safety and good condition of the assets during loading, transportation, and unloading operations.
- The delivery team/logistics service provider maintains a record of asset delivery, specifying (but not limited to) the list of loaded items requiring delivery, asset details and condition, items/assets loaded in the delivery vehicle, and the delivered/unloaded items/assets at the organization's buildings, in addition to the status of asset delivery.
- The department must investigate any discrepancies between the required assets for delivery and the delivered assets and their condition.

Warehouse and Storage Management:

- Warehouse and storage facilities must comply with health and safety standards. The design should be well-organized, and cleaning and internal supervision services should be consistently carried out to prevent damage or accidents during material unloading operations.

- A design/site map should be created, specifying and organizing the sections and storage areas to facilitate access to and identification of assets.
- In line with safety and security policies, warehouse and storage areas should be equipped with visible and accessible fire extinguishers ready for use in case of a fire. Regular monitoring and surveillance should also be conducted.
- Equipment used for loading and unloading assets should be stored in designated areas to ensure easy access when needed.
- The department is responsible for ensuring the recording of all assets issued to and received from the organization's warehouses in the system, ensuring their reconciliation, numbering, and registration for easy tracking and retrieval.
- Any damage occurring during the loading or unloading process should be recorded and reported

Agency Inventory and Fixed Asset Management:

- The department is responsible for receiving all assets and consumables related to the agency's purchases.
- The department handles requests from departments for stationery and consumables, and all requests are updated in the system.
- The department is required to conduct regular inventory reviews (weekly reviews) and coordinate with the procurement team to reorder when inventory levels fall below predefined levels.
- The department is responsible for defining a procurement schedule based on the agency's requirements and conducting regular reviews and updates to meet the agency's needs.
- All received materials must match the purchase order and be entered into the system before storage in the warehouse.
- The General Services Department is responsible for inspecting the materials received from the supplier in terms of quantity and technical specifications to ensure consistency with the purchase order. They notify the supplier of the
- material receipt, store the materials in the designated location, and record the commercial transactions in the system.
- If the received materials do not match the purchase order or any discrepancies are noted, the responsibility falls on the General Services Department, in consultation

with the relevant management, to contact the supplier for returning the products and follow the necessary procedures to receive the correct materials.

- The department is responsible for managing and monitoring the transportation and installation of agency assets, including furniture, equipment, etc.
- Proper labeling should be placed on all fixed assets for identification and tracking purposes. These labels should indicate the type of assets, their numbering, and location. If an asset is entrusted to an employee, the relevant employee data should be added for tracking in coordination with the respective departments (Human Resources, Information Technology).
- A physical verification of assets should be conducted at least once every two years for all agency assets. For this purpose, the management department appoints a team to physically verify the assets, including representatives from the relevant departments (Finance, Internal Audit, and Information Technology).
- The department is responsible for preparing a physical verification report that identifies discrepancies due to losses or damages, and updates the asset register accordingly. The department coordinates with the Finance Department to update the financial details of the assets in the system.

Procedures:

- Facility Management:
  - The General Services team identifies the requirements for property and facility management, including equipment related to fire safety, security, cleaning and maintenance, facility management, and minor civil works. These requirements are then submitted to the General Services Manager.
  - The General Services Manager reviews the maintenance and cleaning requirements and provides feedback to the team for necessary adjustments. Additionally, the department head/lead informs the team of the approved
  - requirements, and the team prepares the scope of facility management and required services.
  - Based on the maintenance and cleaning requirements, as well as the scope of facility management, the team develops a facility management plan. This plan includes identifying activities that can be carried out internally and those that should be outsourced to external entities. It also establishes a schedule for facility maintenance and determines the frequency of maintenance work.

Furthermore, the team establishes a framework for report preparation and monitoring. The facility management plan is then submitted to the General Services Manager for review.

- The General Services team reviews the facility management plan and provides feedback to the team for necessary adjustments. Additionally, the department head/lead submits the management requirements and the plan to the General Services Manager for final review and approval.
- The General Services Manager reviews the facility management requirements and related plans and gives final approval. Subsequently, contracts can be finalized. The manager is required to discuss the facility management plan with suppliers and make final adjustments before initiating the facility management process.
- Based on the preventive maintenance plan and cleaning schedule, the general services team coordinates with the cleaning and maintenance teams to obtain the necessary materials from the organization's warehouse. The general services team must coordinate with the relevant department to carry out specific maintenance tasks, such as IT equipment maintenance, and monitor and supervise the maintenance and cleaning activities.
- After completing the maintenance and cleaning tasks, the maintenance or cleaning team updates the maintenance and cleaning records with the completed work. These records are then submitted to the general services team.
- The general services team reviews the cleaning and maintenance records on a daily basis and inspects the completed work to document any issues and suggest corrective measures as needed. Problems and proposed corrective actions are reviewed, and follow-up is conducted with the relevant teams to find solutions.
- In all cases, the general services team is required to prepare a periodic report related to facility management. The report is reviewed and approved by the General Services Manager and shared with the General Services Manager.

- Health and Safety:
  - The General services team identifies the health and safety requirements and related standards concerning the facilities of the OCA (Health, Safety, and Monitoring Activities). They assess the risks and survey areas of potential hazards.
  - The General Services Manager reviews the risks and health and safety requirements. They provide feedback to the team as needed. Additionally, they notify the team of their approval to prepare the health and safety plan, which addresses the identified risks. This plan includes inspection tasks, required training, health and safety-related communications, and an emergency response plan.
  - The department head/lead reviews the health and safety plan and submits it to the General Services Manager for any necessary modifications. Upon approval, the General Services Manager adopts the health and safety plan and notifies the department head/lead to initiate the "Management of Health, Safety, and Monitoring Activities."
  - During the implementation of health and safety activities, the General services team must monitor the execution of tasks and address any incidents. They should update the relevant details, stakeholders involved, date and time of the incident, and proposed resolutions in the health and safety record.
  - Based on the implementation processes, the General Services Manager prepares periodic health and safety reports. These reports include progress according to the health and safety plan, deviations from the plan, incident data, proposed action plans, and are sent for approval and dissemination.
  - The General Services Manager reviews the health and safety report, approves it, and circulates it to the relevant parties.
  - The General services team conducts inspection and security audits in the workplace, including periodic monitoring of parking areas and workspaces. They inspect fire safety equipment, maintenance, and repairs. Additionally, the
  - team is responsible for conducting fire preparedness drills, testing evacuation plans, and determining health and safety requirements based on training and inspection operations.
  - The General Services Manager reviews the health and safety requirements and provides feedback for any necessary adjustments to the team.

Furthermore, the department head/lead submits the requirements to the General Services Manager for final review and approval.

- The General Services Manager reviews and approves the health and safety requirements. They notify the General Services Manager accordingly, who then coordinates with the Procurement Department to issue a service order if there is an existing contract or as part of a comprehensive purchasing agreement. If there is no existing contract or agreement for the required services, a new purchase request must be submitted, and a process for a new contract should be initiated.
- Upon completing the necessary contract procurement processes, the General services team supervises the replacement, repair, or installation operations related to health and safety. The process of planning, executing, and monitoring health and safety activities takes place.

- Transportation Management:
  - The department or relevant entity within the organization determines the need for transportation or the use of organization vehicles and obtains the necessary approval from the department head/lead/manager.
  - The General Services Manager receives and reviews the request for vehicle usage, ensuring the availability of sufficient justifications. Then, they forward the request to the relevant team for execution.
  - The General Services team verifies the availability of vehicles/usage schedule.
    - If the vehicle is not available, the concerned party is informed about the possibility of using it at a later time.
    - If the vehicle is available, coordination is done with the driver/authorized employee for usage and updating the necessary information in the vehicle usage record. The vehicle usage record includes:
      - Driver/employee details
      - Vehicle details
      - Purpose of vehicle usage
      - Location/destination
      - Pickup time
      - Return time

- After registering the required data, the leader of the relevant team in the General Services delivers the vehicle to the driver or employee.
- The team monitors and reports any breakdowns or accidents to the General Services Manager to take necessary actions with relevant entities (such as traffic authorities, insurance companies, concerned employees, HR department, etc.).
- The team periodically monitors any traffic violations and reports them to the department head/lead to take appropriate measures.

Appendices

Job Descriptions

President

Brief Description:

The President is the overall head of the Olympic Council of Asia (OCA), ensuring compliance with the organization's constitution, overseeing key responsibilities, and embodying the highest standards of leadership. This role involves effective communication, strategic collaboration, and adherence to the OCA's mission, values, OCA Code of ethics, Constitution and OCA Rules and Regulations.

Compliance with OCA Constitution: Ensure strict compliance with the OCA Constitution, upholding its principles and regulations in all organizational activities and decisions.

Compliance with OCA Code of Ethics: Adhere to the OCA Code of Ethics, promoting integrity, transparency, and ethical conduct in all operations, decisions, and interactions, ensuring alignment with the Olympic Movement's values and the OCA's commitment to fair and responsible governance.

Key Responsibilities:

In accordance with the OCA Constitution, OCA Code of Ethics, and in the best interest of the OCA and the Asian Games, the President shall:

- Delegate duties, as necessary, to the Vice President or the CEO/Director General during his/her absence, ensuring seamless and continuous operations while maintaining oversight.
- Oversee all OCA activities, matters, operations, and communication, channeling them through OCA management in strict adherence to the OCA Constitution, rules, and regulations.
- Serve as the First Vice President or participate in other committees as required to support OCA objectives.
- Collaborate with the CEO/Director General to oversee the Asian Games, ensuring compliance with and enforcement of all related rules and regulations, while promoting the event's success and integrity.

Qualifications:

- Proven leadership experience in a comparable role.
- Extensive knowledge of sports governance and the Olympic Movement.
- Excellent understanding of the OCA Constitution and its application.
- Strong diplomatic and communication skills.
- Demonstrated commitment to ethical conduct and integrity.

Competencies:

- Ability to formulate and implement a clear strategic vision for the OCA.
- Inspire and lead a diverse team towards achieving organizational objectives.
- Foster collaboration and positive relationships with internal and external stakeholders.
- Uphold the highest standards of ethics and integrity in all actions.
- Navigate and lead the organization through evolving challenges.

Lines of Communication:

Report directly to the Executive Board, maintaining open and transparent communication channels. Collaborate with committee heads, staff members, and external partners as necessary.

KPIs:

- Ensure effective organizational governance.
- Foster positive relationships with stakeholders.
- Demonstrate strong leadership and team management.
- Uphold the values and mission of the OCA.

CEO/Director General

Brief Description:

The CEO/Director General occupies a critical leadership position within the Olympic Council of Asia (OCA), ensuring strict compliance with the organization's constitution, overseeing all essential responsibilities, and exemplifying the highest standards of professional leadership. This role requires advanced communication proficiency, strategic collaboration, and steadfast commitment to the OCA's mission and core values.

The CEO/Director General serves as the Head of OCA Management, Operations, and Chief of Staff, providing strategic oversight and operational leadership to drive the organization's success.

Compliance with OCA Constitution:

Ensure strict compliance with the OCA Constitution and OCA Code of Ethics, upholding OCA principles and regulations in all organizational activities and decisions.

Key Responsibilities:

In accordance with the Compliance and OCA Constitution and OCA Code of Ethics.

Note: The CEO/ Director General may delegate their duties, as necessary, to Deputy Director General or the Chief Operating Officer (COO), Chief Financial Officer (CFO), or Finance Director/Chief Finance Officer (CFO) during their absence while ensuring smooth and continuous operations.

Qualifications:

- Proven leadership experience in a comparable role, with a minimum of 20 years of demonstrated success in strategic management and organizational leadership.
- Extensive knowledge of sports governance and the Olympic Movement, underpinned by at least 20 years of deep involvement and expertise in the field.
- Exceptional understanding of the OCA Constitution and its practical application, reflecting a thorough mastery of its principles and regulatory framework.
- Outstanding diplomatic and communication skills, with a proven ability to engage diverse stakeholders and foster effective international relations.
- Demonstrated unwavering commitment to ethical conduct and integrity, evidenced by a consistent track record of upholding the highest moral and professional standards.

Competencies:

- Ability to formulate and implement a clear strategic vision for the OCA.
- Inspire and lead a diverse team towards achieving organizational objectives.
- Foster collaboration and positive relationships with internal and external stakeholders.
- Uphold the highest standards of ethics and integrity in all actions.
- Navigate and lead the organization through evolving challenges.

Working Conditions:

The role involves frequent national and international travel, attendance at various sporting events, and engagement in evening or weekend activities as required.

Lines of Communication:

Report directly to the OCA President, ensuring transparent and regular updates on strategic and operational matters. Collaborate with senior leadership (Deputy Director General, COO, CFO, FD), National Olympic Committees, IOC, and external stakeholders, fostering effective communication to advance the OCA's mission.

Key Performance Indicators (KPIs):

- Ensure effective organizational governance.
- Foster positive relationships with stakeholders.
- Demonstrate strong leadership and team management.
- Uphold the values and mission of the OCA.

Support Staff for President and CEO/Director General:

Brief Description:

The support staff for the President and CEO/Director General are integral to the operational success of the Olympic Council of Asia (OCA), providing dedicated administrative, logistical, and security assistance to ensure the effective execution of strategic and operational objectives. Comprising a maximum of three personnel per leader, this team is responsible for managing correspondence, coordinating high-profile events, and safeguarding the safety of the President and CEO/Director General during official engagements. Operating under strict governance guidelines, the staff uphold the OCA's mission and values, delivering professional support while maintaining confidentiality and ethical integrity.

Key Responsibilities:

- The President and CEO/Director General rely on dedicated support staff to facilitate administrative operations, ensuring strategic and operational objectives are met with governance integrity.
- The President and the CEO/Director General of OCA may each have a maximum of three (3) support staff, responsible respectively for:
    - **Secretariat and Administrative Support**: Managing correspondence, scheduling, and documentation to streamline leadership tasks.
    - **Protocol and Logistics**: Coordinating official events, travel arrangements, and protocol requirements to uphold OCA's international standards.
    - **Security and Safety Coordination**: Ensuring the safety of the President or CEO/Director General during official engagements, coordinating with relevant security agencies, and managing risk assessments for events and travel.
- The appointment, employment contracts, and working relationship of these staff members shall strictly follow the provisions of the OCA Constitution (Articles 21), Financial Guidelines & Governance, HR Policy & Procedures, and the OCA Employee Manual.
- These staff members are administrative personnel only and shall not represent the President or the CEO/Director General in any official capacity. They are strictly prohibited from dealing with or communicating on behalf of the OCA with Sports Organizations, National Olympic Committees (NOCs), International Federations (IFs), Asian Federations (AFs), or any third party without prior coordination and written approval from the OCA CEO/Director General.

- All OCA-related travel by these staff members must follow the approved financial and administrative rules of the Council, including travel approvals, per diems, and mission scope.
- These provisions apply equally to the offices of both the President and the CEO/Director General of OCA.
- Confidentiality: Staff maintain strict confidentiality of sensitive information.
- Performance and Oversight: Staff performance is evaluated annually to ensure alignment with governance standards.
- Ethical Conduct: Staff adhere to OCA's ethical standards, avoiding conflicts of interest as per OCA Code of Ethics.

Qualifications:

- Minimum of 5 years of proven experience in administrative support roles, with a focus on organizational management and coordination.
- Minimum of 5 years of demonstrated expertise in protocol, logistics, or security operations, depending on the assigned support function.
- Solid understanding of governance frameworks and policies, including the OCA Constitution and related regulations.
- Strong communication and interpersonal skills, with the ability to maintain professionalism in diverse settings.
- Demonstrated commitment to ethical conduct and integrity, aligned with the OCA Code of Ethics.

Lines of Communication:

The President's staff report directly to the President or CEO/Director General, while the CEO/Director General's staff report to the CEO/Director General, ensuring a structured and efficient reporting hierarchy. Both positions maintain open and transparent communication channels to foster accountability and collaboration.

Working Conditions:

The position entails frequent national and international travel to facilitate official duties, mandatory attendance at various sporting events, and availability for evening or weekend activities as required to ensure seamless support for the President and CEO/Director General. Staff must be prepared to adapt to dynamic schedules and maintain high performance under demanding conditions while adhering to OCA protocols.

Key Performance Indicators (KPIs):

- Ensure efficient administrative support and governance integrity by consistently meeting operational and strategic objectives set by the President and CEO/Director General.
- Foster effective collaboration with internal teams and external partners, strengthening support services and stakeholder engagement.
- Demonstrate reliability and professionalism in team management, contributing to the smooth execution of leadership tasks and responsibilities.
- Uphold the OCA's values and mission through exemplary conduct, maintaining confidentiality and ethical standards in all activities.

Chief Compliance and Ethics Officer

Brief Description:

The Chief Compliance and Ethics Officer plays a crucial role in ensuring adherence to regulatory requirements, ethical standards, and internal policies within the Olympic Council of Asia (OCA). This position involves overseeing compliance initiatives, promoting ethical conduct, and upholding the highest standards of integrity throughout the organization.

Compliance and Ethics Oversight: Lead and manage the implementation of compliance programs, policies, and procedures to ensure adherence to regulatory standards, ethical guidelines, and internal controls.

Key Responsibilities:

- Develop, implement, and oversee comprehensive compliance programs in line with relevant laws, regulations, and industry best practices.
- Conduct regular assessments and audits to identify compliance risks and develop strategies to mitigate these risks effectively.
- Collaborate with departments to provide guidance and training on compliance-related matters, fostering a culture of ethics and integrity.
- Establish reporting mechanisms for ethics violations or breaches of compliance and ensure appropriate investigation and resolution.
- Advise senior management and the Executive Board on compliance issues, emerging trends, and regulatory changes that may impact the organization.
- Serve as a liaison with regulatory bodies, fostering positive relationships and ensuring transparency in communications.

Qualifications:

- Extensive experience in compliance, ethics, or a related field within a comparable organization.

- Strong understanding of regulatory requirements, ethical standards, and compliance frameworks.
- Excellent communication and interpersonal skills to effectively engage and educate stakeholders at all levels.
- Demonstrated ability to develop and implement compliance programs and initiatives.

Competencies:

- Strategic thinking and ability to develop and execute compliance strategies aligned with organizational goals.
- Strong leadership skills to foster a culture of ethics, compliance, and integrity.
- Analytical mindset to assess risks and develop effective risk mitigation strategies.
- Effective communication and negotiation skills in dealing with regulatory bodies and stakeholders.

Lines of Communication:

Report directly to CEO/Director General and maintain open communication channels with relevant departments and stakeholders.

Working Conditions:

The role may involve occasional travel and attendance at relevant industry conferences or regulatory meetings as required.

KPIs:

- Ensure effective implementation and monitoring of compliance programs.
- Reduce compliance-related risks and incidents.
- Establish and maintain a robust ethics and compliance culture within the OCA.

Finance Director / Chief Finance Office (CFO)

Brief description

The Finance Director / Chief Finance Officer will be responsible for managing the financial operations of the Olympic Council of Asia (OCA), ensuring compliance with OCA's Constitution and financial guidelines, and providing accurate and timely financial information to the CEO/DG.

Compliance with OCA Constitution

The Finance Director / Chief Finance Officer of the Olympic Council of Asia (OCA) shall be responsible for managing the financial affairs of the organization in accordance with the OCA Constitution, regulations, and policies. Specifically, the Finance Director / Chief Finance Officer shall ensure compliance with the following clauses and articles of the OCA Constitution:

- Article 18: Financial Control and Audit: The Finance Director / Chief Finance Officer shall be responsible for the preparation of the annual budget and the proper management of OCA's financial affairs. The Finance Director / Chief Finance Officer shall also ensure that proper accounting records are maintained and that the organization's financial statements are audited annually in accordance with internationally accepted standards.
- Article 19: Financial Regulations: The Finance Director / Chief Finance Officer shall ensure that OCA's financial affairs are managed in accordance with the Financial Regulations.
- Article 21: Expenditures: The Finance Director / Chief Finance Officer shall ensure that all expenditures are authorized and in accordance with the approved budget.
- Article 22: Investments: The Finance Director / Chief Finance Officer shall manage OCA's investments in accordance with the Investment Policy.
- Article 23: Bank Accounts: The Finance Director / Chief Finance Officer shall ensure that OCA's bank accounts are managed in accordance with the Financial Regulations.

- Article 24: Reporting: The Finance Director / Chief Finance Officer shall report regularly to the CEO/DG on the financial affairs of the organization.

The Finance Director / Chief Finance Officer shall also ensure compliance with any other relevant clauses or articles of the OCA Constitution or regulations related to financial management and reporting. This includes using predictive analytics to proactively identify potential compliance risks related to Articles 18-23, ensuring robust adherence to governance standards.

Key Responsibilities

- Oversee the financial operations of the OCA, including accounting, budgeting, and financial reporting.
- Develop and maintain financial policies and procedures that comply with the OCA Constitution and applicable laws and regulations.
- Provide accurate and timely financial information to the Executive Board and other stakeholders.
- Manage the OCA's investments and financial assets.
- Ensure compliance with all tax and regulatory requirements.
- Manage relationships with external auditors and ensure that audit requirements are met.
- Develop and maintain effective internal controls to minimize financial risks.
- Manage the financial aspects of contracts and agreements with vendors and suppliers.
- Manage and mentor the finance team.
- Collaborate with the marketing team to align financial strategies with OCA’s sponsorship and marketing regulations (Article 20), ensuring maximum return on investment for partnerships.
- Create and maintain a stakeholder-friendly financial dashboard, accessible via a secure portal, to provide real-time insights into OCA’s financial health for CEO/DG.

Qualifications

- Bachelor's / Master's degree in finance, accounting, or a related field.
- Certified Public Accountant (CPA) or equivalent certification.

- At least 20 years of experience in financial management, preferably in a large organization or government agency.
- Experience in managing investments and financial assets.
- Experience in managing relationships with external auditors.
- Strong knowledge of accounting principles, tax regulations, and financial reporting requirements.
- Excellent analytical and problem-solving skills.
- Strong leadership and interpersonal skills.

Competencies (in order of importance)

- Financial management
- Compliance management
- Strategic thinking
- Leadership
- Communication skills
- Analytical thinking
- Problem-solving
- Risk management

Lines of communication

- The Finance Director / Chief Finance Officer will report to the CEO/Director General.

Working conditions

- The Finance Director **/** Chief Finance Officer will work in a fast-paced and demanding environment, with occasional travel required.

KPI's

- Deliver the monthly financial statements to the Executive Board in a timely manner.
- Maintain a high level of compliance on all audits and reviews.
- Implement cost control measures and track progress monthly to enhance fiscal responsibility.
- Conduct quarterly performance reviews with a focus on continuous improvement.
- Regularly review financial controls and policies to ensure consistent adherence.

- Secure a satisfactory audit rating and adhere to the approved timeline for the audit process.

Legal Advisor

Brief Description

The Legal Advisor is responsible for overseeing all legal matters within the organization, providing legal advice and guidance to senior management and staff, and ensuring compliance with legal regulations and requirements. The Legal Advisor works closely with all departments within the organization to manage legal risks and support the organization's mission and objectives.

Compliance with OCA Constitution

The Legal Advisor of the OCA is responsible for providing legal guidance and support to the organization. In carrying out this role, the Legal Advisor is expected to comply with the OCA Constitution and Regulations, specifically with the following articles:

- Article 2 - Objectives: The Legal Advisor shall ensure that all legal matters of the OCA are handled in accordance with the objectives of the organization as outlined in this article.
- Article 16 - Jurisdiction of the CAS: The Legal Advisor shall be familiar with the jurisdiction of the Court of Arbitration for Sport (CAS) as outlined in this article and shall ensure that all legal matters of the OCA are handled in accordance with the jurisdiction of the CAS.
- Article 18 - Anti-Doping: The Legal Advisor shall be familiar with the anti-doping regulations of the OCA as outlined in this article and shall ensure that all legal matters related to anti-doping are handled in accordance with these regulations.
- Article 19 - Dispute Resolution: The Legal Advisor shall be familiar with the dispute resolution mechanisms of the OCA as outlined in this article and shall ensure that all legal matters related to dispute resolution are handled in accordance with these mechanisms.

- Article 20 - Sanctions: The Legal Advisor shall be familiar with the sanctions that can be imposed by the OCA as outlined in this article and shall ensure that all legal matters related to sanctions are handled in accordance with these provisions.
- Article 21 - Procedural Matters: The Legal Advisor shall ensure that all legal matters related to procedural matters are handled in accordance with the procedures outlined in this article.
- Article 22 - Appeals: The Legal Advisor shall be familiar with the appeals process of the OCA as outlined in this article and shall ensure that all legal matters related to appeals are handled in accordance with this process.
- Article 23 - Statute of Limitations: The Legal Advisor shall ensure that all legal matters related to the statute of limitations are handled in accordance with the provisions outlined in this article.
- Article 24 - Liability: The Legal Advisor shall be familiar with the liability provisions of the OCA as outlined in this article and shall ensure that all legal matters related to liability are handled in accordance with these provisions.

In summary, the Legal Advisor is expected to ensure that all legal matters of the OCA are handled in accordance with the OCA Constitution and Regulations, and specifically with the articles outlined above.

Key Responsibilities

- Provide legal advice and guidance to senior management and staff on a range of legal issues, including contracts, employment law, intellectual property, and compliance with legal regulations.
- Review and draft contracts, agreements, and other legal documents to ensure legal compliance and protect the organization's interests.
- Manage all legal disputes, including litigation and arbitration, and work with external legal counsel as necessary.
- Develop and implement legal policies and procedures to ensure compliance with legal regulations and requirements.
- Manage and maintain the organization's legal records, including contracts, legal correspondence, and other legal documents.

- Provide legal training and support to staff on legal matters.
- Liaise with external legal counsel and other stakeholders, including government agencies and regulatory bodies.
- Monitor and report on legal developments and trends that may impact the organization and advise senior management and staff accordingly.
- Represent the organization in legal proceedings, negotiations, and other legal matters.
- Manage the Legal department budget and resources effectively.

Qualifications

- Law degree from an accredited institution.
- A minimum of 20 years of relevant legal experience, preferably in a sports or nonprofit organization.
- Admitted to practice law in the relevant jurisdiction.
- Excellent knowledge of legal regulations and requirements related to sports organizations and nonprofits.
- Strong analytical and problem-solving skills.
- Excellent written and verbal communication skills.
- Strong leadership and management skills.

Competencies:

- Legal expertise and knowledge
- Attention to detail and accuracy
- Strong communication and interpersonal skills
- Strategic thinking and decision-making abilities
- Leadership and management skills
- Ability to work under pressure and manage multiple priorities

Lines of communication:

- The Legal Advisor reports to the President and CEO/Director General and works closely with all departments within the organization.

Working conditions

- The Legal Advisor typically works in an office environment and may be required to attend meetings and events outside of normal working hours.

KPI's

- Ensure legal compliance of the organization's operations and activities.
- Review and draft all contracts and legal documents within established timelines and quality standards.
- Manage legal disputes and work towards timely resolution.
- Develop and implement legal policies and procedures for compliance with regulations.
- Provide legal training and support to staff, enhancing legal awareness and minimizing risks.
- Manage the Legal department budget and resources effectively.
- Maintain positive working relationships with external legal counsel and stakeholders.
- Provide accurate and timely legal advice and guidance to senior management and staff.
- Monitor and report on legal developments and trends impacting the organization.
- Represent the organization in legal proceedings and negotiations, seeking favorable outcomes where possible.

Director of International & NOC Relations

Brief description

The Director of International & NOC Relations is responsible for leading and managing the organization's international relations and engagement with National Olympic Committees (NOCs), ensuring effective communication and collaboration, and supporting the organization's mission to promote the Olympic values and principles.

Compliance with OCA Constitution

The Director of International & NOC Relations plays a crucial role in ensuring compliance with the Olympic Council of Asia's (OCA) constitution. The following clauses or articles are relevant to the Director's responsibilities:

- Article 10.1 - The Role of the Director of International & NOC Relations
  According to this article, the Director of International & NOC Relations is responsible for developing and maintaining relationships with National Olympic Committees (NOCs) and International Olympic Committee (IOC) members. This includes coordinating and supporting the participation of NOCs in OCA events and activities.
- Article 10.3 - International Relations
  This article requires the Director of International & NOC Relations to promote cooperation and mutual understanding between OCA and other continental and international sports organizations.
- Article 10.4 - NOC Relations
  The Director of International & NOC Relations is responsible for promoting and coordinating the activities of NOCs, including training programs, exchange of technical expertise, and participation in OCA events.
- Article 10.5 - Athlete Relations
  The Director of International & NOC Relations is responsible for promoting and coordinating the activities of athletes, including training programs, exchange of technical expertise, and participation in OCA events.

- Article 23 - Reports

  This article requires the Director of International & NOC Relations to provide regular reports to the OCA CEO/Director General on the activities of the department, including updates on the relationships with NOCs and other organizations.

In summary, the Director of International & NOC Relations is responsible for developing and maintaining relationships with NOCs and other organizations, promoting cooperation and mutual understanding, and coordinating the activities of NOCs and athletes. Regular reporting on these activities is also required. It is important for the Director to ensure compliance with the relevant articles of the OCA Constitution to uphold the integrity and mission of the organization.

Key Responsibilities

- Develop and implement a strategic plan for international and NOC relations that supports the organization's mission and objectives.
- Establish and maintain positive relationships with National Olympic Committees (NOCs), ensuring effective communication and collaboration.
- Coordinate with other functional areas, such as Sports Development and Athlete Performance, Marketing and Sponsorship, and Operations, to ensure integrated and effective delivery of programs and services to NOCs.
- Representing the organization at international events, conferences, and meetings, promoting the organization's mission and values.
- Collaborate with NOCs to support their development and growth, including providing resources, technical assistance, and expertise.
- Develop and implement programs and initiatives that promote the Olympic values and principles and raise awareness of the organization's mission and work.
- Develop and maintain relationships with key stakeholders, including international sports organizations, governments, and other entities, to build a strong network of support for the organization's mission.
- Manage budgets for international and NOC relations programs, ensuring that resources are allocated efficiently and effectively.

- Monitor and evaluate program outcomes to continuously improve program effectiveness.
- Stay up to date with the latest trends and developments in international sports relations to ensure programs remain innovative and effective.

Qualifications

- Bachelor’s degree in international relations, Sports Management, or a related field. Master's degree is preferred.
- Minimum of 20 years of experience in international relations or sports management, with at least 5 years of experience in a leadership role.
- In-depth knowledge of the international sports landscape, including the Olympic movement and National Olympic Committees.
- Excellent communication, interpersonal, and leadership skills.
- Strong project management and budgeting skills.

Competencies

- Strategic thinking and planning.
- Leadership and people management.
- Strong problem-solving skills.
- Excellent communication and interpersonal skills.
- Results-oriented and goal-driven.
- Strong project management skills.
- Flexibility and adaptability to changing situations.
- Innovative and creative mindset.

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.

- Internal Communication: Collaborates with other functional areas, including Sports Development and Athlete Performance, Marketing and Sponsorship, and Operations.
- External Communication: Works closely with National Olympic Committees, international sports organizations, governments, and other entities.

Working conditions

- Office-based, with frequent travel to attend meetings and events.
- Long and irregular working hours, including weekends and holidays, especially during major international events.

KPI's

- Cultivate positive connections with National Olympic Committees and global sports organizations, consistently gauging satisfaction through periodic surveys among NOCs and international sports entities.
- Enhance recognition of the organization's mission and values within critical stakeholders such as NOCs, governments, and related entities.
- Innovate and execute programs fostering Olympic values and principles, contributing to NOC development.
- Effectively manage the international and NOC relations budget, emphasizing streamlined resource allocation.
- Sustain a highly content team within international and NOC relations.

Director of Medical & Anti-Doping

Brief description

The Director of Medical & Anti-Doping is responsible for developing, implementing, and overseeing medical and anti-doping policies and programs for the organization. The position requires a thorough understanding of medical and anti-doping regulations, as well as the ability to provide medical support and guidance to athletes and teams.

Compliance with OCA Constitution

The Director of Medical & Anti-Doping is responsible for ensuring compliance with the OCA Constitution and the World Anti-Doping Code (WADA) regarding medical and anti-doping matters within the Olympic Council of Asia.

The Director of Medical & Anti-Doping must comply with the following articles of the OCA Constitution:

- Article 26: The OCA recognizes the authority of the International Olympic Committee (IOC) Medical Commission and the World Anti-Doping Agency (WADA) in matters relating to medical and anti-doping issues.
- Article 28: The OCA recognizes the principles and regulations of the World Anti-Doping Code and will cooperate with WADA and other organizations in the fight against doping in sport.
- Article 29: The OCA will establish and implement anti-doping rules and procedures consistent with the World Anti-Doping Code and will comply with the anti-doping rules and procedures of the IOC and WADA.
- Article 30: The OCA will establish and implement medical rules and procedures consistent with the principles and regulations of the IOC Medical Commission and will comply with the medical rules and procedures of the IOC.

Key Responsibilities

- Develop and implement medical and anti-doping policies and programs for the organization, in accordance with international and national regulations and standards.
- Provide medical support and guidance to athletes and teams, including injury prevention, diagnosis, and treatment, as well as nutritional and psychological support.
- Manage the organization's medical team, including physicians, physiotherapists, and other medical professionals, ensuring that all medical services are delivered effectively and efficiently.
- Develop and implement anti-doping education and awareness programs for athletes and coaches, to ensure compliance with anti-doping regulations and standards.
- Collaborate with international and national anti-doping organizations, as well as with medical and scientific experts, to stay up-to-date on the latest medical and anti-doping research and developments.
- Conduct regular medical and anti-doping audits and assessments, to ensure that all policies and programs are effective and compliant with regulations and standards.
- Oversee the organization's medical and anti-doping testing programs, ensuring that all testing is conducted in a fair, unbiased, and confidential manner.
- Manage the organization's medical and anti-doping budget, ensuring that all expenditures are within budgetary limits and aligned with organizational priorities.
- Ensure that all medical and anti-doping activities are conducted in accordance with the organization's code of conduct and ethical standards.
- Ensure that all medical and anti-doping activities are properly documented and reported, in accordance with regulations and standards.

Qualifications

- Bachelor's degree in medicine or a related field.
- Postgraduate degree or certification in sports medicine or anti-doping.

- Minimum of 15 years of experience in sports medicine or anti-doping, including at least 5 years in a leadership role.
- Strong understanding of medical and anti-doping regulations and standards, as well as international and national sports organizations.
- Strong leadership, communication, and collaboration skills, with the ability to work effectively with athletes, coaches, medical professionals, and other stakeholders.
- Strong analytical and problem-solving skills, with the ability to make sound decisions based on data and evidence.
- Strong organizational and project management skills, with the ability to manage multiple projects and priorities simultaneously.

Competencies

- Leadership
- Communication
- Collaboration
- Problem-solving
- Strategic thinking
- Attention to detail
- Analytical thinking
- Project management
- Decision-making
- Ethics and integrity

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.
- Collaborate with athletes, coaches, medical professionals, and other stakeholders.
- Collaborates with international and national sports organizations, as well as with medical and scientific experts.

Working conditions

- Office-based with frequent travel required to attend competitions and meetings.
- May be required to work outside of regular business hours, including evenings and weekends.

KPI's

- Increase compliance rate with anti-doping regulations based on annual testing results.
- Increase athlete satisfaction with medical services based on annual survey results.
- Reduce medical and anti-doping budget maintaining the same level of quality and compliance.
- Increase the number of certified anti-doping officials as required through training and development programs.
- Implement a new electronic medical record system for all athletes and medical staff to keep appropriate tracking.
- Decrease the number of anti-doping rule violations through increased testing and education programs.
- Develop and implement a new concussion protocol for all sports.
- Increase the number of medical staff certifications and qualifications through training and development programs.

Director of Media and TV Broadcasting

Brief Description

The Director of Media and TV Broadcasting is responsible for managing the organization's media and broadcasting activities and ensuring the efficient and effective delivery of content to audiences. The role is critical in enhancing the organization's brand and reputation through the creation and dissemination of compelling content that engages audiences across multiple platforms.

Compliance with OCA Constitution

The Director of Media and TV Broadcasting shall perform their duties in compliance with the Olympic Council of Asia Constitution, including but not limited to the following clauses:

- Article 26.5 - The Director of Media and TV Broadcasting shall be responsible for all aspects of the OCA's media and broadcasting operations, ensuring the promotion of the OCA's activities and events through various media channels.
- Article 29.2 - The Director of Media and TV Broadcasting shall provide regular reports to the Director-General on the progress and results of the media and broadcasting operations.
- Article 29.6 - The Director of Media and TV Broadcasting shall work closely with the Director of Marketing and Sponsorship to ensure effective coordination of media and broadcasting activities with marketing and sponsorship programs.
- Article 30.4 - The Director of Media and TV Broadcasting shall oversee the production and dissemination of information and content related to the OCA and its events through various media channels, ensuring accuracy and quality of such content.
- Article 30.5 - The Director of Media and TV Broadcasting shall ensure compliance with all relevant laws and regulations related to media and broadcasting, including those related to intellectual property, copyrights, and trademarks.

The Director of Media and TV Broadcasting shall also uphold the values and principles of the Olympic Movement, including the principles of fair play, non-discrimination, and respect for athletes and their rights.

Key Responsibilities

- Develop and implement a media and broadcasting strategy that supports the organization's strategic objectives and mission.
- Oversee the production and distribution of content across various media platforms, including TV, radio, print, and online.
- Develop and manage budgets for media and broadcasting activities, ensuring that resources are allocated efficiently and effectively.
- Develop and maintain relationships with media partners and stakeholders to maximize coverage and exposure of the organization's activities and events.
- Coordinate with other functional areas, such as Sports Development and Athlete Performance, Marketing and Sponsorship, and International and NOC Relations, to ensure integrated and effective delivery of content.
- Manage and develop a high-performing media and broadcasting team, including hiring, training, coaching, and performance management.
- Monitor and evaluate audience engagement and feedback to continuously improve content quality and relevance.
- Ensure compliance with relevant laws, regulations, and policies, including those related to content creation, copyright, and broadcasting standards.
- Develop and implement processes and systems to improve operational efficiency and effectiveness in media and broadcasting activities.
- Ensure that media and broadcasting activities are aligned with the organization's values and principles, including diversity, equity, and inclusion.

Qualifications

- Bachelor’s degree in communications, Media Studies, Broadcasting, or a related field. Master's degree is preferred.
- Minimum of 10 years of experience in media and broadcasting, with at least 5 years of experience in a leadership role.

- Strong knowledge of media and broadcasting, including content creation, distribution, and audience engagement.
- Excellent communication, interpersonal, and leadership skills.
- Strong project management and problem-solving skills.

Competencies

- Strategic thinking and planning.
- Leadership and people management.
- Strong problem-solving skills.
- Excellent communication and interpersonal skills.
- Results-oriented and goal-driven.
- Strong project management skills.
- Flexibility and adaptability to changing situations.
- Innovative and creative mindset.

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.
- Internal Communication: Collaborates with other functional areas, including Sports Development and Athlete Performance, Marketing and Sponsorship, and International and NOC Relations.
- External Communication: Develops and maintains relationships with media partners and stakeholders.

Working conditions

- Office-based, with occasional travel to attend meetings and events.
- Long and irregular working hours, including weekends and holidays, especially during major international events.

KPI’s

- Develop and implement a media and broadcasting strategy that supports the organization's strategic objectives and mission, achieving alignment between media and broadcasting activities and strategic objectives.
- Oversee the production and distribution of content across various media platforms, including TV, radio, print, and online, achieving more audience engagement rate based on annual surveys and ratings.
- Develop and manage budgets for media and broadcasting activities, ensuring that resources are allocated efficiently and effectively, while maintaining or improving content quality and relevance.
- Develop and maintain relationships with media partners and stakeholders to maximize coverage and exposure of the organization's activities and events, achieving satisfaction rate among partners and stakeholders based on annual surveys.
- Develop and implement processes and systems to improve operational efficiency and effectiveness in media and broadcasting activities, achieving increase in efficiency and a 5% increase in effectiveness annually based on internal evaluations.
- Ensure compliance with relevant laws, regulations, and policies, including those related to content creation, copyright, and broadcasting standards, achieving a compliance rate based on internal and external audits.
- Develop and implement initiatives to promote diversity, equity, and inclusion in media and broadcasting activities, achieving alignment between media and broadcasting activities and the organization's values and principles based on annual audits.
- Develop and maintain a high-performing media and broadcasting team, achieving a minimum employee satisfaction rate based on annual surveys and reduction in employee turnover rate.
- Monitor and evaluate audience engagement and feedback to continuously improve content quality and relevance, achieving improvement in audience engagement and feedback annually based on internal and external evaluations.

- Ensure that media and broadcasting activities contribute to enhancing the organization's brand and reputation, achieving positive media coverage and sentiment based on annual media analysis.

Director of Marketing and Sponsorship

Brief Description

The Director of Marketing and Sponsorship is responsible for developing and implementing marketing and sponsorship strategies that promote the organization's brand, increase revenue, and enhance its reputation. The role involves developing and managing relationships with sponsors, partners, and stakeholders to ensure the delivery of mutually beneficial outcomes.

Compliance with OCA Constitution

The Director of Marketing and Sponsorship of OCA is responsible for developing and implementing marketing and sponsorship strategies to support the organization's goals and objectives. In carrying out their duties, the Director of Marketing and Sponsorship must comply with the following provisions of the OCA Constitution:

- Article 24.2: The Director of Marketing and Sponsorship shall report to the Secretary-General and shall be responsible for the promotion of the Olympic Movement in Asia and the development of marketing and sponsorship programs to support the OCA's mission and objectives.
- Article 24.5: The Director of Marketing and Sponsorship shall establish and manage relationships with sponsors, partners, and other stakeholders to support the OCA's marketing and sponsorship programs.
- Article 24.6: The Director of Marketing and Sponsorship shall develop and implement marketing and sponsorship policies and guidelines to ensure compliance with the Olympic Charter, OCA Constitution, and other applicable regulations.
- Article 24.7: The Director of Marketing and Sponsorship shall coordinate with the International Olympic Committee (IOC) and other National Olympic Committees (NOCs) to develop joint marketing and sponsorship programs that support the Olympic Movement in Asia.
- Article 24.8: The Director of Marketing and Sponsorship shall ensure that all marketing and sponsorship programs are consistent with the Olympic values and

- principles and do not compromise the integrity of the Olympic Movement in any way.
- Article 24.9: The Director of Marketing and Sponsorship shall submit reports on marketing and sponsorship activities to the Executive Board and General Assembly as required.
- Article 24.10: The Director of Marketing and Sponsorship shall ensure that all marketing and sponsorship activities are conducted in a transparent and ethical manner and comply with all applicable laws and regulations.

The Director of Marketing and Sponsorship must also work closely with other directors and senior management team members to ensure that the organization's marketing and sponsorship strategies are aligned with its overall objectives and priorities.

Key Responsibilities

- Develop and implement marketing and sponsorship strategies that align with the organization's goals and objectives, achieving a minimum of 10% revenue growth annually.
- Build and maintain relationships with sponsors, partners, and stakeholders to ensure their ongoing engagement and support, achieving a minimum of 90% satisfaction rate based on annual surveys.
- Develop and manage the organization's brand, ensuring that it is consistently communicated and reflected in all marketing and sponsorship activities, achieving a minimum of 80% brand recognition among the target audience based on annual surveys.
- Develop and manage marketing campaigns and initiatives to promote the organization's programs, events, and initiatives, achieving a minimum of 5% increase in audience engagement annually based on internal and external evaluations.
- Develop and implement sponsorship packages and proposals that align with the organization's values and principles, achieving a minimum of 80% alignment rate between sponsorship packages and the organization's values and principles based on annual audits.

- Manage the organization's online presence, including its website, social media accounts, and email marketing campaigns, achieving a minimum of 10% increase in online engagement annually based on internal and external evaluations.
- Develop and manage marketing and sponsorship budgets, ensuring that they are efficiently allocated and effectively utilized, achieving a minimum of 95% budget utilization rate based on annual audits.
- Provide regular reports and updates to the CEO/Director General and other stakeholders on the effectiveness and impact of marketing and sponsorship activities, achieving a minimum of 90% satisfaction rate based on stakeholder feedback.

Qualifications

- Bachelor’s or master’s degree in marketing, business administration, or a related field.
- Minimum of 15 years of experience in marketing and sponsorship, preferably in the sports industry.
- Strong understanding of marketing principles and practices, including digital marketing, branding, and sponsorships.
- Excellent communication, negotiation, and relationship-building skills.
- Strong project management skills and the ability to manage multiple tasks and priorities.
- Proficiency in Microsoft Office, Adobe Creative Suite, and other relevant software programs.

Competencies

- Strategic thinking and planning
- Relationship building and management
- Creative problem solving
- Results-driven and goal-oriented
- Excellent communication and presentation skills
- Team leadership and management

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.
- Collaborate with other directors and department heads to ensure the alignment of marketing and sponsorship activities with the organization's goals and objectives.
- Works closely with sponsors, partners, and stakeholders to ensure the delivery of mutually beneficial outcomes.

Working conditions

- Work is primarily performed in an office environment.
- May require occasional travel for meetings, events, and sponsor/partner visits.

KPI’s

- Achieve revenue growth annually from marketing and sponsorship activities.
- Achieve satisfaction rate from sponsors, partners, and stakeholders based on annual surveys.
- Achieve brand recognition among the target audience based on annual surveys.
- Achieving an increase in audience engagement annually from marketing campaigns and initiatives.
- Achieve alignment rate between sponsorship packages and the organization's values and principles based on annual audits.
- Achieving an increase in online engagement annually from the organization's online presence.
- Achieve budget utilization rate for marketing and sponsorship activities based on annual audits.
- Achieve satisfaction rate from stakeholders on the effectiveness and impact of marketing and sponsorship activities based on stakeholder feedback.
- Secure more new sponsorship partners per year.

Director of Sports Development and Athlete Performance

Brief Description

The Director of Sports Development and Athlete Performance is responsible for leading and managing the development and implementation of high-performance sports programs, ensuring the delivery of athlete-focused, science-driven, and evidence-based programs that enable athletes to achieve their full potential.

Compliance with OCA Constitution

The Director of Sports Development and Athlete Performance of the OCA shall be responsible for the overall direction, management, and development of sports and athletes within the OCA region. The Director shall comply with the following OCA Constitution clauses and articles:

- Article 11.1.7: To provide and implement programs and plans for the development of sports and athletes.
- Article 11.1.8: To encourage and develop sports science and sports medicine, including anti-doping, coaching, and technical officials.
- Article 11.1.10: To provide opportunities for the participation of athletes from the OCA region in regional and international competitions.
- Article 11.1.12: To promote the welfare and protect the rights of athletes and to ensure that sports and athletes are conducted in a fair and ethical manner.
- Article 11.1.13: To ensure that sports and athletes are free from political, racial, and religious discrimination.
- Article 11.1.14: To promote gender equality in sports and to encourage the participation of women in sports.
- Article 11.1.17: To provide support and assistance to National Olympic Committees and other sports organizations within the OCA region in the development of sports and athletes.

The Director of Sports Development and Athlete Performance shall perform his/her duties in accordance with the OCA Constitution and shall work closely with other OCA officials,

including the CEO/Director General to achieve the goals and objectives of the OCA in the area of sports development and athlete performance.

Key Responsibilities

- Develop and implement long-term athlete development programs that support the growth and performance of athletes.
- Create and manage budgets for athlete development programs, ensuring that resources are allocated efficiently and effectively.
- Identify and recruit talent at all levels of athlete development, including coaches and support staff.
- Provide leadership and guidance to coaches and support staff to ensure consistent delivery of high-performance programs.
- Work closely with National Olympic Committees (NOCs), National Sports Federations (NSFs), and other stakeholders to ensure effective communication and collaboration.
- Ensure that sports programs comply with ethical standards and anti-doping regulations.
- Monitor and evaluate athlete performance and program outcomes to continuously improve program effectiveness.
- Develop and maintain relationships with key stakeholders, including athletes, coaches, and sports organizations, to build a strong network of support for athlete development programs.
- Stay up to date with the latest sports science research and trends to ensure programs remain evidence-based and innovative.
- Collaborate with other functional areas, such as Medical and Anti-Doping and Marketing and Sponsorship, to ensure integrated and effective delivery of athlete development programs.

Qualifications

- Bachelor’s degree in international relations, Sports Management, or a related field. Master's degree is preferred.

- Minimum of 20 years of experience in international relations or sports management, with at least 5 years of experience in a leadership role.
- In-depth knowledge of the international sports landscape, including the Olympic movement and National Olympic Committees.
- Excellent communication, interpersonal, and leadership skills.
- Strong project management and budgeting skills.

Competencies

- Strategic thinking and planning.
- Leadership and people management.
- Strong problem-solving skills.
- Excellent communication and interpersonal skills.
- Results-oriented and goal-driven.
- Strong project management skills.
- Flexibility and adaptability to changing situations.
- Innovative and creative mindset.

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.
- Internal Communication: Collaborates with other functional areas, including Sports Development and Athlete Performance, Marketing and Sponsorship, and Operations.
- External Communication: Works closely with National Olympic Committees, international sports organizations, governments, and other entities.

Working conditions

- Work in a fast-paced, dynamic environment with constantly evolving priorities.
- Willingness to work flexible hours, including evenings and weekends as required to support Asian Games and other sports events.
- May require international travel as part of the role.

KPI's

- Increase revenue generated from major sporting events through the development and implementation of effective marketing and sponsorship strategies.
- Increase athlete participation in the Asian Games over the next four years through the implementation of athlete development programs.
- Ensure full compliance with anti-doping and athlete welfare regulations and guidelines, consistently passing all relevant inspections and audits.
- Implement a comprehensive performance management system for all staff within the Asian & Games Sport Department to enhance employee engagement and retention.
- Successfully deliver major sporting events within the designated timeframe and budget, maintaining a high standard and achieving customer satisfaction.
- Attain a high athlete satisfaction rate concerning the organization and management of Asian Games and other sports events.

Director of Operations

Brief Description

The Director of Operations is responsible for managing the organization's day-to-day operations and ensuring the efficient and effective delivery of programs and services to stakeholders. The role is critical in ensuring that the organization's operations are aligned with its strategic objectives and mission.

Compliance with OCA Constitution

The Director of Operations is responsible for ensuring the efficient and effective operation of the organization's activities in accordance with the OCA Constitution. The following clauses or articles of the OCA Constitution are particularly relevant to the role of Director of Operations:

- Article 4.4: The OCA Executive Board shall delegate responsibilities to the Director of Operations, who shall have the authority to manage the daily affairs of the OCA, including the supervision of personnel, in accordance with the Constitution, Bylaws, and regulations.
- Article 8: The OCA shall carry out its activities in accordance with the principles of the Olympic Charter and the rules and regulations of the IOC.
- Article 15.2: The Director of Operations shall be responsible for the management of the OCA headquarters and shall be responsible for the implementation of the policies and programs approved by the Executive Board.
- Article 17.3: The Director of Operations shall appoint and dismiss the employees of the OCA, subject to the approval of the Executive Board.
- Article 20.1: The OCA shall be responsible for the organization and management of the Asian Games, in accordance with the Olympic Charter, the rules and regulations of the IOC, and the agreements concluded between the OCA and the host city and country.

The Director of Operations must ensure that the organization's activities are carried out in compliance with the OCA Constitution, particularly in relation to the delegation of

responsibilities to the CEO/Director General, adherence to the principles of the Olympic Charter and rules and regulations of the IOC, implementation of policies and programs approved by the Executive Board, appointment and dismissal of employees, and organization and management of the Asian Games. The Director of Operations must work closely with the Chief Operating Officer (COO) and other members of the senior management team to ensure that the organization's activities are carried out efficiently and effectively in compliance with the OCA Constitution.

Key Responsibilities

- Develop and implement an operational plan that supports the organization's strategic objectives and mission.
- Oversee the organization's day-to-day operations, ensuring that programs and services are delivered effectively and efficiently.
- Develop and manage budgets for operations, ensuring that resources are allocated efficiently and effectively.
- Ensure compliance with relevant laws, regulations, and policies, and manage risks associated with operations.
- Develop and maintain relationships with key stakeholders, including sponsors, vendors, partners, and suppliers.
- Coordinate with other functional areas, such as Sports Development and Athlete Performance, Marketing and Sponsorship, and International and NOC Relations, to ensure integrated and effective delivery of programs and services.
- Develop and implement processes and systems to improve operational efficiency and effectiveness.
- Manage and develop a high-performing operations team, including hiring, training, coaching, and performance management.
- Monitor and evaluate program outcomes to continuously improve program effectiveness.
- Ensure that operations are aligned with the organization's values and principles, including sustainability and social responsibility.

Qualifications

- Bachelor’s degree in business administration, Operations Management, or a related field. Master's degree is preferred.
- Minimum of 15 years of experience in operations management, with at least 5 years of experience in a leadership role.
- Strong knowledge of operations management, including budgeting, risk management, and process improvement.
- Excellent communication, interpersonal, and leadership skills.
- Strong project management and problem-solving skills.

Competencies

- Strategic thinking and planning.
- Leadership and people management.
- Strong problem-solving skills.
- Excellent communication and interpersonal skills.
- Results-oriented and goal-driven.
- Strong project management skills.
- Flexibility and adaptability to changing situations.
- Innovative and creative mindset.

Lines of communication

- Report to the Chief Operating Officer (COO) and maintain strong relationships with other functional heads within the organization.
- Internal Communication: Collaborates with other functional areas, including Sports Development and Athlete Performance, Marketing and Sponsorship, and International and NOC Relations.
- External Communication: Develops and maintains relationships with sponsors, vendors, partners, and suppliers

Working conditions

- Office-based, with occasional travel to attend meetings and events.
- Long and irregular working hours, including weekends and holidays, especially during major international events.

KPI's

- Develop and implement an operational plan that aligns significantly with the organization's strategic objectives and mission.
- Oversee the organization's day-to-day operations to ensure effective and efficient delivery of programs and services, maintaining a high satisfaction rate among stakeholders according to annual surveys.
- Develop and manage budgets for operations with a focus on efficient resource allocation, aiming for reduced operational costs while enhancing program outcomes and effectiveness.
- Ensure adherence to relevant laws, regulations, and policies, managing operational risks with a commitment to achieving a high compliance rate based on internal and external audits.
- Foster relationships with key stakeholders, striving for a strong satisfaction rate among sponsors, vendors, partners, and suppliers based on annual surveys.
- Implement processes and systems to enhance operational efficiency and effectiveness, targeting continuous improvement annually based on internal and external benchmarks.
- Lead and develop a high-performing operations team, aiming for a high employee satisfaction rate and reduced turnover based on annual surveys.
- Monitor and evaluate program outcomes for continuous improvement, aspiring to enhance program effectiveness annually based on internal and external evaluations.
- Ensure operational alignment with the organization's values and principles, including sustainability and social responsibility, assessed through annual audits.
- Uphold a high compliance rate with health and safety regulations and policies based on internal and external audits.

HR Manager

Brief Description

The HR Manager is responsible for the overall management of the human resources function within the OCA. This role ensures that the organization's HR policies and procedures are effective, efficient, and compliant with legal and regulatory requirements. The HR Manager is also responsible for the recruitment, retention, and development of a high-performing and diverse workforce that supports the organization's goals and objectives.

Compliance with OCA Constitution

The HR Manager for OCA is responsible for ensuring compliance with the OCA Constitution and regulations related to human resources. Specifically, the HR Manager must ensure that all human resources policies and procedures are in line with the OCA Constitution and regulations, including those related to recruitment, hiring, performance management, and employee relations.

The following articles of the OCA Constitution are particularly relevant to the role of the HR Manager:

- Article 30: Functions of the Secretariat
- Article 32: Appointment of Staff
- Article 33: Service Conditions
- Article 34: Performance Evaluation and Promotion
- Article 35: Discipline and Dismissal
- Article 36: Grievances and Appeals

Overall, the HR Manager is responsible for ensuring that all human resources policies and procedures are in line with the OCA Constitution and regulations, and that all employees are treated fairly and equitably.

Key Responsibilities

- Develop and implement HR policies and procedures that align with the OCA's strategic priorities and are compliant with legal and regulatory requirements.
- Manage the recruitment and selection process for all OCA employees, including job posting, resume screening, interviewing, and reference checking.
- Develop and implement employee retention strategies that promote a positive work environment and encourage employee engagement and job satisfaction.
- Provide guidance and support to department heads and supervisors on HR issues, including performance management, employee relations, and disciplinary procedures.
- Develop and implement training and development programs that enhance the skills and capabilities of the OCA's workforce.
- Manage the compensation and benefits program, ensuring that it is competitive and aligns with industry standards.
- Ensure compliance with labor laws and regulations, including employment contracts, labor agreements, and other legal requirements.
- Maintain accurate and up-to-date employee records, including personnel files and HR databases.
- Conduct regular HR audits to identify areas for improvement and ensure compliance with legal and regulatory requirements.
- Develop and maintain relationships with external HR consultants and vendors to ensure access to the latest HR solutions and services.

Qualifications

- Bachelor’s or master’s degree in business administration, or a related field.
- 15+ years of experience in HR management, preferably in a sports or nonprofit organization.
- Strong knowledge of HR policies and procedures, labor laws and regulations, and compensation and benefits programs.
- Experience with recruitment and selection, performance management, employee relations, and training and development.
- Excellent communication and interpersonal skills.

Competencies:

- Strategic thinking and planning
- Leadership and team management
- Communication and interpersonal skills
- Problem-solving and decision-making
- Adaptability and flexibility
- Attention to detail

Lines of communication:

- Reports to the Finance Director/Chief Finance Officer (CFO)
- Works closely with other directors and department heads
- Liaise with external HR consultants and vendors

Working conditions

- Standard office hours, with the possibility of extended hours during peak periods.
- Some trips may be required to attend conferences, meetings, and training sessions.

KPI's

- Implement effective retention strategies to reduce employee turnover.
- Enhance employee satisfaction through the implementation of engagement programs and initiatives.
- Provide HR services and support that meet the satisfaction of department heads and supervisors.
- Conduct regular audits and assessments to ensure compliance with labor laws and regulations.
- Develop and implement HR policies and procedures aligned with industry best practices and regulatory requirements.
- Enhance workforce diversity through targeted recruitment and selection initiatives.

- Implement training and development programs to improve the skills and capabilities of the OCA's workforce.
- Maintain employee records and HR databases with a high level of accuracy.
- Monitor and control HR budget to ensure expenses are within budgeted limits.
- Ensure employee satisfaction with the compensation and benefits program.
- Implement HR technology solutions to improve the efficiency and effectiveness of HR processes.

Director of Information Technology

Brief Description

The Director of Information Technology (IT) is responsible for setting the strategic direction and overseeing the management, security, and innovation of all technology systems and digital infrastructure across the Olympic Council of Asia (OCA). This role ensures technology alignment with OCA's vision, supports seamless operations, safeguards data, and drives digital transformation across the organization. The IT Director leads the IT department, collaborates with all OCA departments and stakeholders, and ensures compliance with applicable standards, policies, and constitutional mandates..

Compliance with OCA Constitution

The Director of IT shall operate in compliance with the OCA Constitution, with specific responsibility for:

- **Article 19.3(a):** Develop and implement technology strategies that align with OCA's strategic objectives and oversee infrastructure modernization.
- **Article 19.3(e):** Maintain robust communication systems between the OCA Secretariat, NOCs, and affiliated bodies.
- **Article 19.3(f):** Ensure data protection and cybersecurity, safeguarding all OCA digital assets and maintaining confidentiality of sensitive information.
- **Article 19.3(g):** Provide capacity building and technical support for OCA staff and member NOCs.

- **Article 19.3(i):** Collaborate with other departments to identify and implement innovative digital solutions that enhance operational performance.

Key Responsibilities

- Lead the strategic planning, budgeting, and execution of OCA's IT and digital transformation initiatives.
- Oversee all IT operations including infrastructure, cybersecurity, systems, applications, and support services.
- Develop and enforce IT governance frameworks, policies, and procedures aligned with international best practices.
- Ensure business continuity through robust data backup, disaster recovery, and incident response plans.
- Drive the adoption of emerging technologies (e.g., cloud computing, AI, automation) to support OCA's evolving needs.
- Supervise IT teams and external vendors to ensure high-quality, cost-effective services.
- Ensure compliance with data protection, privacy regulations, and OCA's internal security policies.
- Promote digital literacy through training, support, and cross-department collaboration.
- Monitor IT system performance, track KPIs, and provide reports and recommendations to senior leadership.
- Foster strong vendor partnerships and manage service-level agreements (SLAs).

Qualifications

- Bachelor's degree in computer science, Information Technology, or a related field.
- At least 20 years of progressive IT experience, with 5+ years in a senior leadership role.
- Demonstrated experience in IT governance, enterprise systems, and digital transformation.
- Proven track record of managing large-scale IT projects, budgets, and teams.
- Strong understanding of cybersecurity frameworks and risk management.

- Experience working in international, sports, or nonprofit organizations is an asset.

Competencies:

- Strategic and analytical thinking
- Enterprise architecture and infrastructure management
- Cybersecurity leadership
- Project and change management
- Strong interpersonal and stakeholder engagement skills
- Budgeting and vendor management
- Effective communication and cross-functional collaboration

Lines of communication:

- The Technology and IT Manager reports to the Chief Operating Officer (COO) and works closely with all departments within the organization.

Working conditions

The Technology and IT Manager typically works in an office environment and may be required to attend meetings and events outside of normal working hours.

KPI’s

- Ensure the smooth and efficient operation of the organization's technology infrastructure, minimizing system downtime or outages.
- Develop and implement IT policies and procedures to uphold the security, integrity, and availability of the organization's data and systems.
- Lead the development and implementation of new technology initiatives to enhance efficiency and productivity, consistently introducing significant initiatives.
- Manage the IT department budget and resources effectively, avoiding significant overspending or underspending.

- Ensure compliance with relevant laws and regulations related to technology and IT, preventing major breaches or violations.
- Maintain positive vendor relationships and contracts related to IT services and products.
- Stay informed about emerging technologies and trends in the IT industry, advising senior management on their potential impact on the organization.
- Ensure effective communication and collaboration with all departments within the organization regarding technology and IT matters.
- Develop and maintain a disaster recovery plan ensuring business continuity in the event of a system failure or outage.
- Enhance system availability by implementing and maintaining a robust and resilient IT infrastructure.
- Realize cost savings in the IT budget through effective resource management and vendor negotiations.

Asian Games Technology Lead

Brief Description:

The Asian Games Technology Lead is responsible for leading the planning, coordination, and implementation of all technology operations related to the Asian Games. This role ensures the delivery of reliable, secure, and integrated technology services across all functional areas of the Games, including venue infrastructure, timing and scoring systems, accreditation, communications, cybersecurity, and digital platforms. The Technology Lead acts as the primary liaison between the OCA, the Host City Organizing Committee, technology partners, and internal stakeholders, ensuring that all technology components are delivered in line with OCA standards and timelines.

Key Responsibilities:

- Lead the end-to-end planning and execution of the Asian Games technology strategy under the guidance of the Director of IT.

- Coordinate with the Host City's Organizing Committee and relevant stakeholders to align technology architecture, infrastructure, and operational readiness.
- Oversee the deployment of key technology services including:
    - Network and communications infrastructure
    - Accreditation and access control
    - Cybersecurity and data protection
    - Broadcasting and media technologies
    - Digital platforms and mobile applications
- Monitor project milestones, timelines, budgets, and risk registers for all technology workstreams.
- Ensure robust testing, simulation, and readiness planning across all venues and systems.
- Support operational delivery during Games-time and coordinate response to any technology-related incidents.
- Ensure technology compliance with OCA's policies, standards, and constitutional obligations.
- Provide ongoing progress reports and post-event documentation for knowledge transfer and future improvements.

Qualifications:

- Bachelor's degree in information technology, Computer Science, Engineering, or related field.
- Minimum of 10 years' experience in managing technology for major sporting or multi-venue international events.
- Proven experience in leading cross-functional technology teams and complex IT deployments.
- Strong understanding of network infrastructure, system integration, cybersecurity, and venue technology.
- Experience with technology coordination in an Olympic or regional games environment is highly desirable.
- Excellent communication, negotiation, and stakeholder management skills.

- Willingness to travel and work on-site during pre-Games, Games-time, and post-Games periods.

Core Competencies:

- Leadership and team coordination
- Project and program management
- Crisis and incident response
- Technology strategy and execution
- Communication and stakeholder engagement
- Attention to detail and risk awareness
- Ability to operate under pressure and tight timelines

Reporting and Communication Lines:

- Reports directly to the Director of Information Technology (IT) at OCA.
- Works closely with:
    - Host City Organizing Committee Technology Team
    - OCA Sports, Accreditation, Media, Protocol, and Operations departments
    - Vendors, NOCs, International Federations, and broadcast partners

Working Conditions:

- Combination of office-based and on-site work at Games venues.
- Extended work hours during pre-Games testing and Games-time operations.
- Frequent travel required, especially in the 12–18 months leading up to the Games.

Key Performance Indicators (KPIs):

- Successful delivery of technology systems across all venues and operations.
- Minimal downtime or disruptions during competition periods.
- Timely and budget-aligned implementation of all technology-related milestones.
- Full compliance with cybersecurity and data protection protocols.
- Positive stakeholder feedback on technology readiness and performance.
- Completion of post-Games technology report and lessons learned.

Network & Infrastructure Lead

Brief Description:

The Network & Infrastructure Lead is responsible for planning, deploying, and maintaining all networking and IT infrastructure components supporting the Asian Games. This includes data centers, venue connectivity, communication systems, Wi-Fi, broadcasting backbones, server rooms, and disaster recovery systems. The role ensures high availability, performance, and security of infrastructure services across all competition and non-competition venues. The Lead will coordinate closely with the Games Organizing Committee, OCA IT, technology partners, and vendors to ensure seamless connectivity and robust infrastructure readiness.

Key Responsibilities:

- Design and oversee the implementation of the Games-wide network architecture, including WAN, LAN, Wi-Fi, VPN, and VLAN setups across all venues and facilities.
- Ensure the scalability, security, and resilience of all IT infrastructure components, including data centers, cloud services, and backup systems.
- Coordinate infrastructure and network deployment across all venues, media centers, command centers, and administrative facilities.
- Lead the configuration, testing, and maintenance of routers, switches, firewalls, and other core infrastructure components.
- Collaborate with cybersecurity teams to ensure secure network configurations and threat mitigation.
- Develop documentation and network diagrams for architecture, operations, and failover planning.
- Supervise infrastructure-related vendors, ensuring compliance with performance standards and SLAs.

- Monitor network performance and availability in real time during the event and ensure rapid incident response.
- Participate in technical rehearsals, simulations, and post-Games decommissioning.
- Provide technical input on procurement, vendor selection, and service level monitoring.

Qualifications:

- Bachelor's degree in Computer Engineering, Network Administration, or related field.
- Minimum of 8–10 years of experience in network and infrastructure management, with at least 3 years in large-scale or multi-venue environments.
- Strong technical knowledge of enterprise networking (Cisco, Juniper, or similar), structured cabling, and infrastructure management tools.
- Experience with redundancy, load balancing, failover, and disaster recovery architecture.
- Understanding of broadcasting and media networking standards is a plus.
- Relevant certifications such as CCNP, CCIE, or CompTIA Network+ are highly desirable.
- Ability to lead cross-functional teams in high-pressure environments.
- Strong documentation, communication, and problem-solving skills.

Core Competencies:

- Technical expertise in network design and troubleshooting
- Infrastructure deployment and site readiness
- Security-first approach to networking
- Vendor and SLA management
- Operational discipline and documentation
- Team coordination and communication

Reporting and Communication Lines:

- Reports directly to the Director of Information Technology (IT) at OCA.

- Works closely with:
    - Games Organizing Committee infrastructure teams
    - OCA IT & Cybersecurity team
    - Venue operations, broadcast, timing, and accreditation teams
    - External technology vendors and ISPs

Working Conditions:

- Field-based work during setup and Games-time operations across multiple venues.
- May require working extended hours, including weekends and nights, during deployment and event periods.
- Travel to venues for infrastructure inspection, testing, and maintenance is expected.

Key Performance Indicators (KPIs):

- Timely delivery and operational readiness of network and infrastructure at all venues.
- High availability and performance of network services during the Games.
- Zero major incidents related to infrastructure failure or security breaches.
- Compliance with OCA standards, policies, and documentation requirements.
- Positive feedback from stakeholders and vendors on infrastructure reliability.
- Accurate and complete technical documentation and post-event reporting.

Systems & Services Lead

Brief Description:

The Systems & Services Lead is responsible for planning, deploying, and managing all core applications and IT services supporting the Asian Games. This includes Games Management Systems (GMS), accreditation systems, results and timing systems (in collaboration with partners), workforce systems, helpdesk platforms, cloud services, and user access management. The role ensures that all systems are functional, integrated, secure, and ready to support operations across venues, command centers, and functional areas throughout the lifecycle of the Games.

Key Responsibilities:

- Lead the planning, configuration, testing, and deployment of all Games-related systems and applications, in alignment with OCA standards.
- Oversee the setup and operations of core platforms such as:
  - Games Management Systems (e.g., registration, scheduling, reporting)
  - Accreditation and access systems
  - Workforce and volunteer management tools
  - Helpdesk and incident management systems
  - Identity and access management (IAM) systems
  - Web services and digital collaboration tools
- Ensure all systems are integrated, secure, and accessible by authorized users across departments and venues.
- Work closely with the network, infrastructure, and cybersecurity teams to ensure system availability and protection.
- Coordinate with vendors, the Host City Organizing Committee, and internal stakeholders to align on configurations, user access, and testing procedures.
- Lead user acceptance testing (UAT), training sessions, and documentation efforts.
- Provide support during Games-time operations, ensuring all systems function reliably under live conditions.
- Monitor system performance, manage escalations, and coordinate resolution of any service disruptions.
- Contribute to post-Games system decommissioning and lessons learned reporting.

Qualifications:

- Bachelor's degree in Information Systems, Computer Science, or related field.
- Minimum of 8 years' experience in IT systems management or enterprise application deployment, preferably in a multi-site or event-based environment.
- Strong understanding of enterprise systems, SaaS/cloud-based applications, and system integration principles.
- Experience with access control, accreditation, workforce systems, or Games Management Systems is highly desirable.
- Excellent organizational, documentation, and user training skills.
- Familiarity with service delivery models, user support, and incident management best practices.
- Certifications such as ITIL, Microsoft, or cloud platforms (e.g., Azure, AWS) are a plus.

Core Competencies:

- System configuration and deployment
- Service delivery and user support
- Cross-functional coordination
- Documentation and training
- Integration and testing oversight
- Incident and change management
- Attention to detail and user-centric thinking

Reporting and Communication Lines:

- Reports directly to the Director of Information Technology (IT) at OCA.
- Works closely with:
    - Network & Infrastructure Lead
    - Cybersecurity team
    - Host City Organizing Committee IT departments
    - Functional area owners (accreditation, workforce, logistics, etc.)

- Software vendors and service providers

Working Conditions:

- Office-based with regular travel to venues and command centers during preparation and event phases.
- May require working irregular hours during testing, deployment, and Games-time operations.
- Availability during critical operational windows and escalation situations is essential.

Key Performance Indicators (KPIs):

- Timely and successful deployment of Games-related systems across all relevant areas.
- High system availability and minimal downtime during the Games.
- Positive user feedback on system usability and support.
- Effective training and onboarding for system users across departments.
- Compliance with OCA policies, cybersecurity standards, and data governance.
- Comprehensive post-Games system documentation and closure reporting.

Procurement & Contract Manager

Brief Description

The Procurement & Contract Manager will be responsible for overseeing all procurement activities and contracts for the OCA. This includes sourcing suppliers, negotiating contracts, and ensuring compliance with all relevant policies and regulations. The successful candidate will have excellent negotiation skills, strong attention to detail, and experience in managing procurement processes.

Compliance with OCA Constitution

The Procurement & Contract Manager will be responsible for ensuring compliance with the following articles of the OCA Constitution:

Article II: Objectives and Functions
Article IV: Management Structure
Article IX: Finance and Audit

Key Responsibilities

- Develop and implement procurement policies and procedures in line with OCA objectives and functions.
- Manage the procurement process from sourcing suppliers to negotiating contracts.
- Ensure compliance with all relevant laws, regulations, and policies.
- Monitor supplier performance to ensure delivery of high-quality goods and services.
- Maintain accurate records of all procurement activities.
- Provide training and guidance to staff on procurement policies and procedures.
- Develop and manage relationships with suppliers and stakeholders.
- Ensure compliance with financial policies and regulations related to procurement

Qualifications

- Bachelor's degree in business administration, Supply Chain Management, or related field.
- Minimum of +10 years of experience in procurement and contract management.
- Experience working in a complex, international organization.
- Strong knowledge of procurement regulations and policies.
- Strong negotiation skills.
- Excellent verbal and written communication skills.
- Ability to manage multiple priorities and meet deadlines.
- Proficiency in Microsoft Office suite and procurement software.

Competencies (in order of importance):

- Strong negotiation skills
- Attention to detail
- Excellent communication skills
- Time management skills
- Analytical thinking and problem-solving skills

Lines of communication

- The Procurement & Contract Manager will report directly to the Finance Director/Chief Finance Officer (CFO) and work closely with other departments within the organization.

Working conditions

- The Procurement & Contract Manager will work in an office environment and may be required to travel occasionally.

KPI's

- Enhance efficiency in the procurement process from requisition to contract award.
- Ensure strong adherence to contract requirements.
- Sustain a high average supplier performance rating.
- Realize cost savings through effective negotiations.
- Uphold a consistently accurate inventory.

General Services Manager

Brief Description

The General Services Manager is responsible for managing all administrative and logistical operations for the Olympic Council of Asia (OCA). They ensure that all necessary resources are secured, efficiently utilized, and that all administrative and logistical functions are in place to support the OCA's mission.

Compliance with OCA Constitution

The General Services Manager for OCA is responsible for providing leadership and management in the areas of office administration and logistics. The Manager must ensure compliance with the OCA Constitution, particularly the following clauses:

Article 3: Objectives and Functions of the OCA

The General Services Manager must ensure that the organization's administrative and logistical functions align with the objectives and functions outlined in Article 3 of the OCA Constitution.

Article 7: OCA Headquarters

The General Services Manager is responsible for the management of the OCA Headquarters, ensuring compliance with all regulations outlined in Article 7 of the OCA Constitution.

Article 12: Committees

The General Services Manager must provide support to the various committees established by the OCA in accordance with Article 12 of the OCA Constitution. This includes logistical and administrative support, as well as ensuring compliance with any regulations or requirements set forth in the Constitution.

Article 22: General Administration

The General Services Manager is responsible for overseeing the general administration of the OCA in accordance with Article 22 of the OCA Constitution, including the management of personnel, facilities, and resources.

In summary, the General Services Manager must ensure compliance with all relevant articles and clauses of the OCA Constitution related to office administration and logistics and provide support to various committees and the general administration of the organization.

Key Responsibilities

- Develop and implement administrative and logistical policies and procedures for the OCA
- Manage all aspects of logistics, including transportation, warehousing, and inventory management for the OCA's events and activities
- Coordinate and oversee facilities management, including maintenance, repairs, and renovations for the OCA's offices and events
- Manage travel arrangements and accommodation for OCA staff and officials during events and meetings
- Develop and manage the OCA's administrative and logistics processes and ensure compliance with relevant regulations
- Develop and manage the OCA's budget for administrative and logistical operations

Qualifications

- Bachelor's degree in business administration, logistics management, Facility Management or related field
- Minimum of 15 years of experience in administration and logistics management, preferably in a sports-related organization
- Strong knowledge of logistics, transportation and operations
- Excellent organizational and communication skills
- Ability to work under pressure and meet tight deadlines

- Strong problem-solving and decision-making skills

Competencies

- Strong leadership and management skills
- Excellent communication and interpersonal skills
- Ability to work in a team-oriented environment
- Proficient in MS Office and logistics management software
- Detail-oriented with strong analytical skills
- Strong negotiation and conflict resolution skills

Lines of communication

- Reports to the Finance Director/Chief Finance Officer (CFO)
- Works closely with other directors and department heads

Working conditions

- Standard office hours, with the possibility of extended hours during peak periods.
- Some trips may be required to attend conferences, meetings, and training sessions.

KPI’s

- Formulate and execute comprehensive administrative and logistical policies and procedures for the OCA.
- Oversee and control all logistical aspects, including transportation, warehousing, and inventory management, for OCA's events and activities.
- Coordinate and supervise facilities management, encompassing maintenance, repairs, and renovations for both OCA offices and events.
- Handle travel arrangements and accommodation for OCA staff and officials during events and meetings.
- Develop and administer administrative and logistical processes for the OCA, ensuring adherence to relevant regulations.
- Manage the budget for administrative and logistical operations within the OCA.

Finance Manager

Brief description

The Finance Manager for OCA is responsible for providing financial leadership, strategic direction, and operational management for the organization. The Finance Manager will be responsible for overseeing the accounting, finance, budgeting, and forecasting functions of the organization.

Compliance with OCA Constitution

The Finance Manager will ensure that all financial operations and decisions are in compliance with the OCA Constitution and applicable laws and regulations.

Key Responsibilities

- Oversee and manage the organization's financial operations including accounting, financial reporting, budgeting, forecasting, and cash management.
- Develop and manage the organization's financial plan, including annual budgets and long-term financial forecasts.
- Analyze financial data and trends to identify areas for improvement and to support decision-making.
- Identify and manage financial risks facing the organization and develop and implement risk management strategies and policies.
- Ensure compliance with financial regulations and laws.
- Develop and implement financial policies and procedures to ensure effective financial governance.
- Build and maintain relationships with key stakeholders including investors, banks, and financial institutions.
- Provide financial guidance and support to the Finance Director/Chief Finance Officer (CFO).
- Manage the finance team and provide leadership, coaching and development opportunities.

Qualifications

- Bachelor's degree in finance, Accounting, Business Administration or related field. MBA or CPA preferred.
- 15+ years of experience in financial management, with at least 10 years in a senior leadership role.
- Strong analytical and financial modeling skills.
- Excellent communication, presentation, and interpersonal skills.
- Knowledge of financial regulations and laws.
- Strong leadership and management skills

Competencies (in order of importance)

- Strategic thinking and planning
- Financial analysis and management
- Risk management
- Compliance and governance
- Leadership and people management
- Communication and interpersonal skills

Lines of communication

- The Finance Manager will report to the Finance Director/Chief Finance Officer (CFO) and will work closely with other senior management team members. The Finance Manager will also work closely with external stakeholders including banks, investors, and financial institutions.

Working conditions

- The Finance Manager typically works in an office environment but may be required to travel occasionally to attend meetings or conferences. The Finance Manager may be required to work long hours to meet deadlines or during peak periods.

KPI's

- Submit financial reports promptly within the specified business timeframe at the end of each month for internal and external stakeholders, including the OCA Finance Director/Chief Finance Officer (CFO) and audit committee, while maintaining a high level of accuracy in the next fiscal year.
- Conduct quarterly reviews of financial controls and policies to ensure effectiveness in the next fiscal year.
- Maintain a cash reserve equivalent to at least three months of operating expenses and implement a monthly cash flow tracking system in the next fiscal year.
- Conduct an annual review of tax compliance with a focus on adherence and accuracy.
- Process all payments promptly upon receipt, ensuring error-free transactions for all financial operations.
- Achieve a forecast accuracy rate and complete all forecasts on time in the next fiscal year.
- Attain a satisfactory audit rating and adhere to the approved timeline for completing the audit process in the next fiscal year.
- Complete the annual financial statements and audit promptly at the end of the fiscal year, aiming for minimal errors per statement.

Legal Manager

Brief Description

The Legal Manager is responsible for providing legal leadership, strategic oversight, and operational management of all contract-related matters and legal affairs. The Legal Manager ensures compliance with contractual obligations, mitigates legal risks, and supports the organization's strategic objectives through robust legal governance.

Compliance with OCA Constitution

The Legal Manager ensures that all contracts, legal agreements, and related activities comply with the OCA Constitution, OCA Code of Ethics, and applicable national and international laws and regulations.

Key Responsibilities

- Draft, review, negotiate, and manage contracts, including sponsorship agreements, vendor contracts, event hosting agreements, and partnership deals, ensuring alignment with OCA objectives.
- Provide legal advice to the Finance Director/Chief Finance Officer (CFO) and senior management on contract terms, compliance, and risk mitigation strategies.
- Identify, assess, and manage legal risks associated with contracts and organizational activities, developing policies to minimize exposure.
- Ensure compliance with all relevant legal and regulatory frameworks, including sports governance, intellectual property, and data protection laws.
- Develop and implement legal policies and procedures to strengthen governance and contract management processes.
- Maintain accurate records of all contracts and legal documents, ensuring accessibility and confidentiality.
- Collaborate with external legal counsel, stakeholders, and partners (e.g., National Olympic Committees, sponsors, and host cities) to resolve legal disputes or issues.
- Support the Finance Director/Chief Finance Officer (CFO) in financial transactions requiring legal oversight, such as funding agreements or procurement contracts.

- Lead and mentor the legal team, fostering professional development and ensuring high performance.

Qualifications

- Bachelor's degree in law (LLB) or equivalent; advanced degree (LLM) or relevant legal certifications preferred.
- 20+ years of experience in contract law, corporate law, or sports governance, with at least 10 years in a leadership role.
- Strong expertise in drafting, negotiating, and managing complex contracts.
- In-depth knowledge of sports governance, international regulations, and the Olympic Movement.
- Excellent communication, negotiation, and interpersonal skills.
- Proven ability to manage legal risks and ensure compliance with regulatory frameworks.

Competencies

- Contract drafting and negotiation
- Legal risk management
- Compliance and governance
- Strategic thinking and problem-solving
- Leadership and team management
- Communication and stakeholder engagement

Lines of Communication

The Legal Manager reports directly to the Finance Director/Chief Finance Officer (CFO) and collaborates closely with senior management. The Legal Manager engages with external stakeholders such as legal counsel, National Olympic Committees, sponsors, and regulatory bodies to ensure effective contract execution and compliance.

Working Conditions

The Legal Manager typically works in an office environment but may require occasional national or international travel to attend contract negotiations, OCA events, or legal

proceedings. Flexible hours, including evenings or weekends, may be necessary to meet deadlines or address urgent legal matters.

Key Performance Indicators (KPIs)

- Draft and finalize all contracts within agreed timelines, ensuring approval without revisions in the next fiscal year.
- Resolve all legal disputes or contract issues promptly, minimizing financial or reputational impact in the next fiscal year.
- Maintain a centralized contract database with full accuracy and accessibility for audits in the next fiscal year.
- Ensure no non-compliance incidents related to contracts or legal obligations in the next fiscal year.
- Complete all legal reviews for financial agreements promptly upon receipt, ensuring error-free documentation in the next fiscal year.
- Achieve a satisfactory rating in annual legal audits, adhering to approved timelines in the next fiscal year.

Revision History:

Revision Date	Change Made	Author
23rd May 2023	P&P Draft version	AlMarsa
16th Nov 2023	P&P Final version	OCA – Internal Audit team
14th April 2024	P&P Revised Final Version	OCA – Internal Audit Team
29th June 2025	P&P & JD's Revised Final Version	OCA – Internal Audit Team

Summary:

The Olympic Council of Asia's Policies and Procedures Handbook serves as a guiding framework, aligning our operations with ethical, transparent, and efficient standards. Upholding the values of integrity, excellence, and inclusiveness, this handbook ensures consistency, compliance, and adherence to the highest standards within our organization.

Reminder:

Every member of the OCA community is encouraged to familiarize themselves with the policies outlined in this handbook. By collectively adhering to these guidelines, we reinforce our commitment to excellence, fairness, and unity in advancing the Asian sporting community.