1.1 SECURITY OPERATION ASSISTANTS (5 positions)

Job Summary

Reporting to the Systems Security Officer, the job holder will be responsible for monitoring the IT infrastructure and supporting investigation of security breaches and incidence response, and perform security impact analysis in the change process.

Key Tasks and Responsibilities

System & Data Access: Maintain access rules to ICT systems and resources including applications and data and ensuring appropriate access control procedures are adhered to meet defined security standards while maintaining supporting documentation, and that access is based on least privilege and need basis, towards maintaining confidentiality and integrity of data.

Systems Security & Change Management: Liaise with the systems analysts, systems design, and systems development teams to provide security design review and approval for new Sacco ICT systems and/or services as well as proposed changes to existing systems and/or services. Further work is to carry out security tests on the systems before deployments.

ICT Disaster Recovery (DR) Planning: Ensure development and maintenance of current DRPs that ensure systems' resilience to support ongoing Sacco operations. Further is to ensure ongoing testing of system backups through scheduled or ad hoc restoration exercises involving business systems owners' signoff and making and recommending relevant adjustments to the plans as may be necessary in order to be within stipulated & expected timelines and thresholds (i.e. RPO, RTO etc.).

Information Security Incident Management: Be involved in the establishment of mechanisms for information and cyber security incident response management including monitoring, detecting, remediating and fully investigating security breaches to establish and treat the root cause (s) so as to minimize future occurrences as well as perform impact analysis.

Risk Assessment and Audit: Proactively monitor current and emerging information and cyber security risks and changes to laws and regulations that may present new business risks, and to detect weaknesses in the design and implementation of controls, carry out vulnerability assessment and penetration testing on Sacco's ICT systems, report identified weaknesses and follow-up on corrective action and its effectiveness. Further, is to engage and support internal and external auditors in their assignments and subsequently assist in laying effective remedial plans to resolve audit findings touching on information and cyber security matters including

reporting on progress of corrective action. Required to Perform malware analysis and digital forensic investigations.

Information & Cyber Security Awareness and Training: Design, recommend and carry out Information and Cyber Security awareness and training campaigns for all Sacco stakeholders/constituents towards creating a culture of consciousness about information and cyber security risks and the different ways in which to avoid or mitigate such risks.

Compliance Monitoring: Ensure compliance with the approved policy, best practice, security requirements and set minimum baseline standards. Document and research security breaches and assess any damage caused.

Professional Development: Grow and maintain professional development by attending educational workshops/seminars/conferences, reviewing professional publications, establishing professional networks and participating in professional societies.
Continuously research on emerging threats and vulnerabilities in information security to gain awareness of the latest information security technologies and developments.

Partners: Assess external partners such as vendors' and contractors' procedures, processes and security controls to ensure they adequately protect the organization's business information and transactions.

Collaboration: Work with user departments to ensure information technology threats are properly identified, analyzed, communicated, investigated and corrective actions taken.

Qualifications

- Bachelor's degree in Information Technology, Computer Science or any other related field with relevant IT Security professional qualifications i.e. CISSP, CISA/CISM/CEH or other relevant security certifications.
- At least 3 years' experience in Security/Network administration with strong technical knowledge of database, network and operating systems security.
- Knowledge of various security methodologies and processes and technical security solutions (firewall and intrusion detection systems).
- Knowledge of TCP/IP Protocols, network analysis, and network/security applications.
- Working knowledge and experience in penetration testing and vulnerability assessments.
- Knowledge of common cybersecurity threats and sources of cybersecurity information.
- Good understanding and knowledge of risk assessment, risk procedures, security assessment, vulnerability management, penetration testing.