STIMA SACCO

... Empowering members for life

1.1 SYSTEMS SECURITY OFFICER

Job Summary

Reporting to the ICT Manager, the job holder will be responsible for Protecting computer assets by establishing and enforcing system controls and maintaining disaster recovery preparedness. Enforcing System Security controls as per ICT Policy and internationally recognized standards and best practices.

Key Tasks and Responsibilities

Security Management (70%)

- ✓ Ensure secure access to information, completeness, accuracy and privacy.
- ✓ Enforce ICT Security Policy.
- ✓ Monitor systems against breaches, data and income leaks 24-7
- ✓ Research, develop, implement, test and review an organization's information security in order to protect information and prevent unauthorized access
- ✓ Assist Risk and Audit team with security related investigations.
- ✓ Establish system controls by developing framework for controls and levels of access.
- ✓ Ensures authorized access by investigating improper access; revoking access; reporting violations; monitoring information requests.
- ✓ Test backups regularly, developing procedures for source code management and disaster preparedness
- ✓ Develops security awareness by providing orientation, educational programs, and on-going communication.
- ✓ Providing expert, timely, and relevant advice to the ICT Manager about computer system security issues and activities affecting the organization.
- ✓ Championing security efforts towards compliance with regulatory standards and Best Practice.
- ✓ Preparation of reports on continued security status of ICT infrastructure and provide remediation measures where vulnerability exists to ensure no adverse threats/impacts affects the systems availability and security for possible financial loss.
- ✓ Supervise the review of technical security assessments of computing environments to identify points of vulnerability, ethical hacking, penetration tests, non-compliance with established Information Security standards and regulations, and recommend mitigation strategies

- ✓ Continuously research on emerging threats and vulnerabilities in information security to gain awareness of the latest information security technologies and developments.
- ✓ 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.
- ✓ Work with user departments to ensure information technology threats are properly identified, analyzed, communicated, investigated and corrective actions taken.
- ✓ Develop and maintain a continuous professional development (CPD) program for the staff in the Section in liaison with the ICT Manager and Human Resource.

Other (20%)

- ✓ The post-holder may under the direction of the ICT Manager assist with the implementation of ICT related projects.
- ✓ Maintain relationships with ICT Support teams and Business
- ✓ Any other duties as may be identified by the ICT Manager.

Qualifications

- Bachelor's degree in IT/ Computer Systems design/ Computer Science or IT related field;
- 5 years of experience practical, proven, hands on experience in IT security from a financial institutions including Sacco's MFIs and Banks;
- Possess professional qualification of Certified Information Security Manger (CISM), and CISA or either Certified Risk and Information System Control (CRISC) and other related field;
- Investigation skills, Knowledge and ability to identify information security breaches;
- Ability to establish an information security monitoring system, Programming skills
- Cyber Security: Digital forensic, malware analysis
- Certificates in Penetration Testing, Vulnerability Assessment
- CEH, CHIF, CISSP or equivalent is an added advantage
- Web Applications Security, Network security or equivalent is an added advantage
- Boot camp (CEH, Ninja Ethical Hacking) with experience is an added advantage