

ICT SECURITY MANAGER:**(1 post)**

	JOB PROFILE
Job Title:	ICT SECURITY MANAGER
Job Reference	TSCCS/ICT.S.M.1/10/2026
Department:	ICT
Reporting to:	HEAD OF ICT
Location	HEAD OFFICE
	JOB PURPOSE
The ICT Security Manager is responsible for establishing, operating and continuously improving Tower SACCO's information and cybersecurity controls across infrastructure, applications, digital channels, data, endpoints, networks and third-party integrations. The position combines cybersecurity governance, security operations, vulnerability management and ethical testing, identity and access management, application and API security, incident response, technology risk management, regulatory compliance and vendor security oversight.	
	JOB DESCRIPTION
(a) Security Governance, Risk and Compliance ➤ Develop, implement and maintain the SACCO's Information Security Management framework, policies, standards, procedures and security baselines in alignment with approved ICT governance and enterprise risk requirements. ➤ Ensure compliance with applicable Kenyan legal and regulatory requirements, including the Data Protection Act, 2019 and relevant guidance/requirements from regulators and oversight bodies applicable to SACCO operations. (b) Security Operations & infrastructure Protection: ➤ Oversee security configuration, monitoring and continuous hardening of servers, endpoints, databases, network infrastructure, virtualization platforms and security appliances across Head Office, branches and disaster-recovery environments. ➤ Administer and continuously review security controls for firewalls, VPNs, WAN connectivity, network segmentation, endpoint protection, anti-malware, email security, web filtering and other security platforms. ➤ Ensure secure configuration and hardening of Windows Server, Oracle Linux, Oracle database environments, VMware infrastructure and other critical enterprise platforms in accordance with approved baselines. (c) Identity, Access and Privileged Access Management ➤ Oversee identity and access security across Active Directory and business applications, including joiner-mover-leaver controls, privileged accounts, service accounts, authentication standards and periodic access reviews. ➤ Enforce least privilege, segregation of duties, multi-factor authentication and strong authentication controls for critical systems, remote access, administrative functions and digital platforms. ➤ Lead implementation and continuous improvement of privileged access management (PAM), network access control (NAC) and related identity-security controls. (d) Application, Digital Channel, API and Secure Change Assurance	

- Ensure security is embedded in the acquisition, development, configuration, integration, testing, change and deployment of ICT systems before and after go-live.
- Conduct or coordinate security reviews, vulnerability assessments and penetration tests for the Core Banking System, mobile banking, internet banking, USSD, agency banking, digital onboarding, digital lending, payment interfaces, APIs and other member-facing or internally critical platforms.
- Assess API and integration security, including authentication, authorization, encryption, credential/secret handling, input validation, session management, transaction integrity, audit trails and exposure of sensitive system information.

(e) Vulnerability Management and Security Testing

- Establish a risk-based vulnerability-management programme covering internal and external assets, applications, databases, network devices and digital services.
- Conduct or coordinate vulnerability assessments, penetration testing, controlled adversary simulation and configuration reviews in accordance with approved scope and rules of engagement.
- Validate and prioritize findings based on business impact, exploitability and exposure; assign remediation actions and track them to closure.

(f) Incident Response, Resilience and Disaster Recovery:

- Lead the technical response to cybersecurity incidents, including detection, triage, containment, eradication, recovery, evidence preservation, root-cause analysis and post-incident improvement actions.
- Maintain and test cybersecurity incident-response procedures and escalation paths, ensuring coordination with the Head of ICT, Risk, Management, vendors and other stakeholders as required.
- Ensure cybersecurity requirements are incorporated into business continuity, backup and disaster-recovery arrangements, including protection against ransomware, unauthorized alteration and loss of critical data.
- Participate in DR/failover exercises and verify security controls, access, logging and system integrity during failover and fallback activities.

(g) Third-Party, Vendor and Technology Supply-Chain Security

- Assess cybersecurity risks arising from core banking, channel, network, cloud, hardware, software and other technology vendors and integrations.
- Define minimum security requirements for technology procurements, contracts, integrations and support arrangements, including access control, data protection, incident notification, vulnerability remediation and auditability.
- Monitor vendor remote access and privileged support activities and ensure access is authorized, time-bound, traceable and reviewed.

(h) Data Protection, Monitoring and Security Awareness

- Implement and monitor controls that protect member, employee and SACCO information from unauthorized disclosure, alteration, loss or misuse, including encryption and appropriate data-loss prevention controls.
- Coordinate cybersecurity awareness initiatives, phishing simulations and targeted sensitization for staff, privileged users and other relevant stakeholders.
- Provide practical security guidance to ICT and business teams and promote a culture of timely reporting of suspicious activity and security incidents.

	PREFERRED QUALIFICATIONS
	➤ Bachelor's degree in Computer Science, Information Technology, Cybersecurity, Information Systems or a related field. ➤ Professional certification in information/cybersecurity such as CISM, CISSP, CISA, CEH, CCNA Cybersecurity/Cyber Ops, CCSP or an equivalent recognized certification. A combination of governance and hands-on technical security certification is an added advantage. ➤ Minimum five (5) years of relevant ICT experience, with at least three (3) years of demonstrable responsibility in information/cybersecurity, security operations, infrastructure security, technology risk or related functions. ➤ Practical experience securing enterprise networks, Windows/Linux servers, Active Directory, databases, virtualization environments, endpoints, firewalls/VPNs and business applications. ➤ Experience in vulnerability assessment, penetration testing, incident response, access-control reviews and remediation management. ➤ Experience within financial services, SACCOs, banking, payments or another regulated environment is a strong advantage. ➤ Working knowledge of recognized security frameworks and good practice such as ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls and OWASP principles is desirable. ➤ KCSE minimum qualifications: (C Plain) with C (plain) in English and Mathematics
	PERSON SPECIFICATIONS
	▪ Age above 30 years. ▪ High integrity, discretion and strong ethical standards when handling privileged access, security information and sensitive member data. ▪ Strong analytical, critical-thinking, problem-solving and troubleshooting capability, including performance under high-pressure incident situations. ▪ Ability to translate technical risks into clear business impact, priorities and actionable recommendations for management and non-technical stakeholders. ▪ Strong knowledge of authentication, authorization, security administration, network and application security, operating-system hardening and vulnerability management. ▪ Understanding of ethical hacking, threat modelling, attack paths and defensive controls, with disciplined adherence to approved scope and responsible disclosure practices. ▪ Strong interpersonal and stakeholder-management skills with the ability to work effectively across ICT, Risk, Internal Audit, business departments and external vendors. ▪ Good planning, documentation and reporting skills, with the discipline to maintain evidence, registers, remediation trackers and security procedures. ▪ Continuous-learning mindset and ability to keep abreast of emerging cyber threats, technologies and regulatory expectations.

DISCLAIMER

The above information on this description has been designed to indicate the general nature and level of work performed by employees within this classification. It is not designed to contain or be interpreted as a comprehensive inventory of all duties, responsibilities and qualifications required of employees assigned to this job.

Candidates who will have applied will receive an email informing them whether they will proceed or not to the next recruitment level of being shortlisted /interviewed.