



HR/STAFF/VAC – 07/01/2026/1

CAREER OPPORTUNITY – HEAD, INFORMATION SECURITY

Responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected within compliance and risk perspectives of the business.

KEY ACCOUNTABILITIES:

- Oversees the development, implementation and enforcement of Cyber and technology policy programs at UGAFODE
- Ensuring that information systems meet the needs of the institution, and the ICT strategy, in particular information system development strategies, comply with the overall business strategies, risk appetite and ICT risk management policies of the institution.
- Ensures that UGAFODE maintains an up-to date enterprise-wide knowledge base of its users, devices, applications, software licenses and their relationships including but not limited to: Software and hardware asset inventory, Network maps (including boundaries, traffic and data flow) and network utilization & performance data.
- Designs cybersecurity controls with the consideration of users at all levels of the institution, including internal (management & staff), external users (contractors/consultants, business partners and service providers).
- Organizing professional cyber related trainings to improve technical proficiency of staff.
- Ensures that regular and comprehensive cyber risk assessments are conducted within the institution.
- Ensures adequate processes & tools are in place for monitoring IT systems to detect cyber and technology events and incidents in a timely manner.
- Conducts reviews associated with exceptions/deviations to the approved cyber and technology policies and procedures and gain senior management approval for risk assessments.
- Assessment of the confidentiality, integrity and availability of the information systems in the institution
- Reporting as agreed on the assessment of the effectiveness of the approved cybersecurity program, all material cyber and technology events that affected the institution, e.t.c.
- Timely detection and action to identify compromises to the IT systems and controls and speedy rectification to avoid financial and operational losses.
- Ensuring the bank's cyber security controls and procedures are up to date to prevent breaches of the bank's systems by internal and external actors.
- Continuously test disaster recovery and Business Continuity Plans (BCP) arrangements to ensure that the institution can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.
- Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.

KNOWLEDGE, SKILLS AND EXPERIENCE REQUIRED:

- Minimum of Bachelor's degree in Computer Science, MIS or equivalent, and any IT certification (e.g. CISCO Certified Network Associate (CCNA) etc.
- At least 6 years' experience in information security or banking computer systems
- Extensive knowledge of Information security within Banking environment including related statutory IT compliance regulations, IT and MIS banking policies & procedures, e.t.c.
- Specialist security certifications such as GSEC (GIAC Security Essentials), CISSP (Certified Information Systems Security Professional) or related field is an added advantage
- Experience with incident response, risk assessment, and management.
- Maintain relevant industry, information technology, and process knowledge expertise
- Ability to maintain confidentiality
- Experience in leading teams
- Exceptional planning and organizational skills, and excellent written and oral communication
- Analytical mind with the ability to quickly get to the root cause of issues
- An overall understanding of relevant scripting and source code programming languages, such as C#, C++, .NET, Java, Perl, PHP, Python and others that are in use.
- An up to date working knowledge of IT Security related hardware, software and vendor solutions.

HOW TO APPLY:

If you believe you meet the requirements as stated above, submit an application letter together with an up-to-date CV to our email: recruitment@ugafode.co.ug. Save the Documents as **Your Full Name** & indicate the job title you are applying for in the Email Subject Line. Your applications should be addressed to the Head of Human Resources and the closing date for receiving all applications is **12th January 2026**.

Note: UGAFODE provides equal opportunity in employment to all people and therefore, women are encouraged to apply