JOB DESCRIPTION

HR2 REV0209

Job Title	Assistant Manager Cyber & Information Security	Job Reference No.	
Department	Operations & IT	Created / Revised	August 2024
Reports to	Assistant Vice President – Operations & IT	Staff Supervised	0

Type of position:	☑ Full-time ☐ Part-time ☐ Contractor ☐ Intern	

RESPONSIBILITIES:

Cyber and Information Security:

- Collaborate with the AVP Ops & IT to develop and implement the Strategic Direction/Plan for cyber security initiatives, ensuring alignment with overall business objectives and IT department goals.
- Develop and maintain standard operating procedures (SOPs) and incident response plans for security incidents, with a focus on continuous review and evaluation to ensure these processes remain effective and aligned with current security standards.
- Monitor security alerts and events from various sources including security information and event management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS), and endpoint protection platforms (EPP), to promptly identify and mitigate potential threats.
- Conduct in-depth analysis of security events and incidents to accurately identify and evaluate potential threats, vulnerabilities and impacts.
- Respond to security incidents in a timely manner, following established procedures and protocols.
- Investigate security breaches, incidents, and unauthorized access attempts, documenting findings and remediation actions taken.
- Collaborate with cross-functional teams to implement security controls, configurations, and best practices to mitigate risks.
- Perform regular security assessments and audits to identify and address gaps and weaknesses in the security posture.
- Maintain and update security tools, technologies, and systems to ensure optimal performance and effectiveness.
- Stay up to date with the latest cybersecurity threats, trends, and technologies to continuously improve CCI's cyber security capabilities.
- Ensure that Cyber Security training is developed and delivered to all CCI's relevant stakeholders to enhance awareness and compliance.
- Develop and report on Cyber Security metrics, providing updates to the AVP Ops & IT and COO at established times.

Administrative:

- **Team Guidance and Support**: Provide guidance and support to members of the IT team, as needed.

- **Operational Oversight**: Plan, organize, direct, control and evaluate the operations of the information systems focusing on optimizing the security and functionality of both hardware & software components.

- **Service Level Management**: Collaborate with the senior leadership team, to propose, discuss, agree and deliver IT services to defined Service Level Agreements - system requirements, specifications, costs and timelines.

- **Budget Management:** Develop and manage the IT Budget under the guidance of the AVP Ops & IT, to ensure prudent and prioritized expenditure.

- **Vendor and Contractor Management**: Oversee the selection and management of vendors and contractors, ensuring the integration of their tasks and the review of their deliverables, specifically in relation to enhancing cyber security.

- **Procurement Support**: Partner and provide support as required to the AVP Ops & IT in the procurement of IT hardware, software and attendant maintenance agreements, ensuring that all contracts with vendors/suppliers/contractors are appropriately executed.

- **Policy Development and Compliance**: Provide strong support to the AVP Ops & IT to develop, implement and ensure compliance with CCI's IT Policies across all offices.

KNOWLEDGE & SKILLS REQUIREMENTS

- **Cyber Security Expertise and Principles:** Profound knowledge of security protocols, cyber laws, information security standards, and frameworks, coupled with a strong understanding of cyber security principles, techniques, and best practices.
- **Strategic Thinking**: Ability to develop and execute strategic plans for cyber security within the broader IT strategy.
- **Analytical Skills**: Strong capability to analyze security systems, interpret alerts, and identify vulnerabilities and potential threats.
- **Incident Response and Analysis**: Proficiency in developing incident response plans and effectively handling security breaches, coupled with the ability to conduct in-depth analysis of security incidents, including packet capture and malware analysis, to identify underlying threats and vulnerabilities.
- **Technical Proficiency with Security Technologies**: Knowledge of current technologies and IT systems, particularly in cyber security, including proficiency with SIEM, IDS/IPS, EPP, firewalls, and vulnerability management tools.
- **Team Leadership and Support**: Skills in leading, guiding, and supporting IT team members to enhance their performance and knowledge in cyber security.
- **Project Management**: Experience in planning, directing, and coordinating IT projects, including handling timelines, budgets, and resource allocation.
- **Communication Skills**: Excellent verbal and written communication skills to effectively interact with all levels of the organization and external stakeholders.
- **IT Policy Development and Compliance**: Skill in developing IT policies and ensuring compliance across the organization to maintain high security and operational standards.
- **Problem Solving**: Strong problem-solving skills to quickly address and resolve IT issues while ensuring minimal impact on operations.
- **Familiarity with Industry Frameworks:** Knowledge of industry frameworks and standards such as NIST, ISO 27001, and CIS Controls.

- **Adaptability and Continuous Learning**: Ability to adapt to rapidly changing technology landscapes and a commitment to continuous learning in cyber security trends and practices.

EXPERIENCE REQUIREMENTS

- A minimum of 3-5 years of experience in the management of cyber and information security systems within the Financial Services sector.
- Demonstrated experience working in a Security Operations Center (SOC) or similar environment.

EDUCATION AND CERTIFICATION REQUIREMENTS

- A bachelor's degree in Computer Science, Information technology, Management or a related field from an accredited institution
- Relevant industry certifications such as CISSP, CEH, GCIH, or equivalent.