Cyber Security Officer
Corporate Services

Position Summary

Reporting to the Manager, Technology Infrastructure & Client Support, the Cyber Security Officer will be responsible for developing and implementing information security, cybersecurity, and Information Technology (IT) risk management programs and tools in order to ensure the secure operation and protection of the organization's internal and external technology systems. Providing direction to the IT Team, including the IT Director, this position will work collaboratively with internal and external stakeholders and third-party providers on the implementation of new security solutions, participation in the creation and/or maintenance of policies, standards, baselines, training programs, guidelines and procedures as well as vulnerability management and compliance audits and assessments.

Key Responsibilities

- Lead and ensure the delivery of an effective corporate-wide information and cyber security program for the organization.
- On behalf of the organization and the entire IT team, develop and manage the frameworks, processes, tools and consultancy necessary to properly manage IT risk and make risk-based decisions related to IT activities.
- Develop strategies, goals and priorities relating to information protection and cyber security operations across the organization, ensuring alignment with divisional and corporate direction.
- Works independently with third-party resources to research, design, implement and provide ongoing management of tools and technologies in support of enhancing overall security program.
- Develop, implement, maintain/manage and oversee ongoing enforcement of policies, procedures, standards, guidelines, controls and trainings for ongoing system security administration, risk mitigation, user awareness and system access based on industry-standard best practices.
- Leads the delivery of the Information Security Program, including Security Vulnerability Management, Incident Response, Threat Management and Monitoring, Risk Reporting, Privacy, Data Security and Security program initiatives.
- Direct, maintain and improve security processes, security playbooks, documentation, practices and measures as a lead of the security team.
- Perform ad-hoc and scheduled internal security compliance checks, reviews, and audits of IT systems to ensure alignment with established operating procedures, standards and guidelines.
- Maintain up-to-date baselines for the secure configuration and operations of all organizational-owned hardware and software assets.
- Maintain operational configurations of all in-place security solutions as per established baselines.
- Monitor all in-place IT security solutions for efficient and appropriate operations, apply configurations, hotfixes and updates as required.
- Coordinate the continuous development, implementation and updating of security and privacy policies, standards, guidelines, baselines, processes and procedures in compliance with applicable organizational risk frameworks, legislation and/or industry best practices.
- Lead the implementation of proof of concept toolsets to improve cyber security response and overall posture of the organization.
- Lead the management, deployment, integration and configuration of all new security solutions and enhancements to existing IT security solutions in accordance with standard best practice procedures.
- Provide recommendations, guidance and security/risk evaluation of all net new technology acquisitions within the organization.

- Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, best practices, improved processes, and the development of new attacks and threat vectors.

Education and Experience

- Post-secondary degree or diploma in Information Technology, Cyber Security, Computer Science or Engineering or related degree is required; Master's Degree is preferred.
- Minimum of five (5) years of broad and progressive information security experience in an enterprise environment.
- Certified Information Systems Security Professional (CISSP) is required.
- Experience with cyber security risk, compliance, and policy development is required.
- Certifications in one or more of the following additional areas Certified Information Systems Auditor (CISA), and/or SANS GIAC Security Essentials (GSEC), and/or Qualified Security Assessor (PCI-QSA or AQSA (Associate)) is an asset.
- Demonstrated knowledge of IT process, control and risk frameworks; specifically, ITIL, COBIT, CIS CSC, NIST, SOC Type 2 and PCI DSS.
- Demonstrated experience with conducting and leading enterprise-wide security assessments, investigations and audits; designing and implementing security controls as necessary to protect information assets and lower organizational risk.
- Advanced knowledge of DNS, DHCP, network topologies and types (WAN, SD-WAN, LAN, WLAN, VLAN, VPNs) as well as the application of secure network design.
- Strong understanding of network firewall auditing and policy design, load balancers, SIEM, SOAR, EDR/XDR, IDPS infrastructures and technologies as well as patch/vulnerability toolsets and processes.
- Advanced knowledge of security auditing and best practice implementation for Active Directory, Azure AD, Office 365, SQL, Exchange, WSUS, IIS, etc.

Salary Range: $97,783 - $122,228 (effective July 1, 2023, based on a 35-hour work week)

This role will be posted until it is filled.

In accordance with the Freedom of Information and Privacy legislation, applicant information is collected under the authority of the Municipal Act and will be used strictly for candidate selection.