CITY OF
PRINCE GEORGE

ROLE DESCRIPTION

JOB TITLE: **CYBERSECURITY LEAD**

DEPARTMENT: **FINANCE AND IT SERVICES**

SCHEDULE: **EXEMPT**

JOB SUMMARY:

Reporting to the Manager, IT Services, the Cybersecurity Lead is responsible for establishing and maintaining an organization wide Cybersecurity management program to ensure that information and technology assets are adequately protected. The Cybersecurity Lead is responsible for assessing the organization’s cyber security posture against common standards and frameworks; developing and leading cybersecurity roadmap activities and projects and serves as the business owner of all cybersecurity related activities including cyber incident response and mitigation plans, cyber security best practices, organizational cyber security policies and administrative procedures, and monitoring / management of key cyber security technologies. A key element of the position is working with management to determine acceptable levels of risk for the organization.

ORGANIZATIONAL STRUCTURE:

The Cybersecurity Lead reports to the Manager, IT Services.

NATURE AND SCOPE:

The incumbent leads the development and execution of an effective and sustainable organizational Cybersecurity program that includes Information Technology (IT) and Operational Technology (OT). He/she facilitates cyber security risk assessments and risk management processes and procedures. The Cybersecurity Lead creates and maintains Cybersecurity standards, policies, administrative procedures, and plans and ensures consistent application of policies, administrative procedures and standards across all IT and OT technology projects, systems and services. The incumbent leads reporting of Cybersecurity KPIs, events, risks, and mitigations and advises senior management and stakeholders.

The incumbent develops, deploys, and maintains Cybersecurity incident response plans and processes, and leads and coordinates cyber incident response activities and resources. He/She develops, maintains, promotes, monitors and reports on Cyber Security Awareness programs across the organization. The incumbent leads the management and maintenance of cyber security awareness training and testing systems and leads the management and maintenance of cyber security monitoring systems and investigates and reports on security alerts.

He/She leads the management and maintenance of data audit and ransomware mitigation systems and investigates and reports on security alert. The incumbent leads the management and maintenance of privileged access management systems and services. The incumbent provides secondary support in the management and maintenance of cyber security systems and services including patch management, anti-spam, security certificates, endpoint security and others as assigned.

The Cybersecurity Lead establishes and implements a regular external Cybersecurity audit including penetration testing and physical access review of IT and OT systems and facilities. He/She performs pro-active threat hunting exercises and provides expertise and/or coordinates resources to track down and mitigate threats and threat origins. The incumbent researches, evaluates, monitors and assesses emerging cyber security threats and risks and develops solutions to mitigate / address.

The incumbent liaises with other relevant internal stakeholders, organizations, and external agencies, to ensure that the organization maintains a strong security posture and is kept abreast of identified threats identified. He/she leads tabletop and live fire disaster recovery testing and identifies / leads any necessary changes to processes and documentation to ensure efficient and effective disaster recovery. He/she plans, organizes, directs, monitors various teams including cyber security advisory committees, cyber incident response teams and other ad-hoc teams and committees as needed.

The Cybersecurity Analyst assists with preparation and management of operating and capital budgets and leads procurement for Cybersecurity-related purchases. He/She leads Cybersecurity related capital and operational projects and/or provides cybersecurity expertise for technology related projects. He/She provides specialized expertise, consulting and training to city staff and stakeholders. The incumbent stays informed on the latest security and technology developments. Develops and maintains cyber security related documentation.

CONTACTS:

The Cyber Security Analyst has significant contact with various levels of management and staff within the organization as well as from external agencies and other government bodies. The incumbent is expected to act in a proactive manner within the City organization. There is a strong emphasis on communication and on building and maintaining positive, professional relationships with both internal and external customers.

EDUCATION / TRAINING

Degree in Computer Science or recognized equivalent. Possession of Certified Information Systems Security Professional certificate (CISSP), Certified Information Security Manager (CISM), and familiarity with the National Institute of Standards and Technology (NIST) framework are considered assets. Five years’ experience in the information technology field, with a broad range of exposure to systems, networks, applications, and database technologies.

Critical Attributes include:

- Good knowledge and understanding of common information and industrial security and IT management frameworks, including ISO.IEC 27001, ITIL, COBIT, NIST, ICS security frameworks.
- Demonstrated knowledge of common Cybersecurity management frameworks, regulatory requirements, and industry leading practices such as Freedom of Information and Protection of Privacy Act.
- Exceptionally strong analytical and problem-solving skills with a strong knowledge and understanding of threat, vulnerability and risk management procedures and processes.
- Good knowledge and understanding of various security related / security reliant technologies including; server and endpoint operating systems, cloud computing services including Software as a Service (SAAS) and Infrastructure as a Service (IAAS), Managed Detection and Response (MDR), Security Information and Event Management systems (SIEM), Security Orchestration, Automation and Response (SOAR), Intrusion Detection systems (IDS), Firewalls, security patching systems, anti-malware, multi-factor authentication (MFA), Virtualization software, backup and restore systems and recovery strategies, systems monitoring and reporting software, authentication protocols, and encryption technologies.
- Ability to work with highly confidential and sensitive information/evidence, exercising sound judgement to make decisions in complex and confidential situations.
- Demonstrated tact, integrity, and diplomacy.
- Demonstrated commitment to customer service excellence.
- Ability to work within, and contribute to, a collaborative team environment.
- Excellent communication abilities and the ability to communicate effectively and professionally, both orally and in writing, specifically the ability to prepare and present presentations of a specialized / highly technical nature.
- Demonstrated Project Management experience.
- Demonstrated initiative and the ability to work independently.
- Strong time management and organizational abilities.
- Ability to deal courteously, tactfully, and diplomatically with co-workers, staff, partners, vendors, and stakeholders.

Driver’s License:	Yes.
Vehicle Usage:	No.
Police Information Check:	Yes. As a condition of employment, the incumbent must be able to obtain and maintain a Police Information Check

Prepared by: B McCloskey/ S Young
Date prepared: February 2023