Job Description

Position Identification			
Position Title	IT Security Analyst I		
Position Replaces	n/a		
Position Level	Employee	**Position Code**	1947
Pay Group	Group 9	**Date (last revised)**	Sep-23
Supervisor Title	Manager, IT Security and Compliance	**Sup. Position Code**	1626
Additional Requirement	TMA	CRC	
Division	Information Technology	**Flexible Work Arrangement**	Flexible Work

Organizational Description

BC Transit is a provincial crown corporation responsible for the overall planning and delivery for all of the different municipal transportation systems within British Columbia, outside Greater Vancouver.

Our Mission: Delivering transportation services you can rely on

Department Summary

The IT Security & Compliance team plays a critical role in safeguarding BC Transit's information assets. We achieve this through developing & enforcing security policies, security architecture design, real-time security monitoring, security awareness training, and collaboration & communication.

Job Overview

Reporting to the Manager, IT Security and Compliance, the IT Security Analyst I is responsible for collaborating with a group of cyber security specialists who are proficient in all elements of technology and cyber security. This role will perform forensic analysis, investigation, and troubleshooting to locate, fix, and report cyber security-related problems. This includes performing threat simulations to identify potential risks and offer remediations, as well as doing risk analysis and analyzing mitigation solutions for cyber security vulnerabilities. Incumbents will also be able to examine and resolve issues with a variety of security platforms, including firewalls, identity management systems, and endpoint detection and response (EDR), etc.

Key Accountabilities and Expectations

Key Accountability	Expectation
Technology	• Maintain and implement technical security controls and processes in support of BC Transit's Information Security Management System • Monitor computer networks and systems for threats and security breaches • Investigate security breaches and other cybersecurity incidents • Work with the SOC (Security Operations Center) team to investigate flagged events • Install security measures and operate software to protect systems and information infrastructure • Detect and mitigate vulnerabilities (network, OS, web and on-prem applications, etc.) • Handle OS and applications patch management process for compliance • Contribute in the development to company-wide best practices for IT security and compliance • Support Internal and external security audits and penetration testing activities • Provide support for end users for all in-place security solutions • Maintain up-to-date baselines for the secure configuration and operations of all in-place devices • Contribute to the maintenance and enhancement of the enterprise's security awareness training program • Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures) • Stay up-to-date on IT security trends including awareness of new or revised security solutions and threat vectors • Monitoring, review, and handle security related ITSM tickets and escalate as required.
Additional Duties	• Performs related duties in keeping with the purpose and accountabilities of the job

Summary of Qualifications and Job Specific Competencies	
Education	• Post secondary diploma in IT Security or a related field. • Completion or in the process of completing one or more of the following certifications: • CompTIA Security+ • GIAC Information Security Fundamentals (GISF) • ISACA Cybersecurity Fundamentals • Microsoft Certified: Security, Compliance, and Identity Fundamentals • ISC2 Certified in Cybersecurity (CC)

Experience	• One-year related experience in managing enterprise level information security or in a related role • An equivalent combination of education and experience may be considered • Experience with security concepts such as MFA, Server Patching, Endpoint/Server Protection, and Access Management • Experience with IT service management such as configuration, change and incident management, and Incident Response Life cycle
Key job-specific competencies	• Knowledge of network segmentation, VLANs, and enterprise networks in the context of cybersecurity along with strong understanding of IP, TCP/IP, and other network administration protocols • Knowledge of IT security best practices, processes, frameworks, and tools • Knowledge of Active Directory and Azure AD (Entra ID) configurations, as well as common Operating Systems such as: Windows (client/server), Linux, and Mac • Familiarity with cloud services such as Azure in the context of security and compliance • Familiarity with IDS/IPS, DLP, security event monitoring, vulnerability assessment, ACLs, and IT forensics • Ability to conduct research into IT security issues and products as required • Ability to effectively prioritize and execute tasks in a high-pressure environment • Strong investigative, analytical, and problem-solving skills • Highly self-motivated and directed • Excellent written, oral, and interpersonal communication skills • Keen attention to detail • Strong team-player and skilled in working within a collaborative environment