Job Description

Position Identification			
Position Title	Intermediate IT Security Analyst		
Position Replaces	N/A		
Position Level	Employee	**Position Code**	2080
Pay Group	Group 11	**Date (last revised)**	Jun-25
Supervisor Title	Manager, IT Security and Compliance	**Sup. Position Code**	1626
Additional Requirement	CRC	TMA	
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 Intermediate IT Security Analyst is responsible for protecting BC Transit’s digital infrastructure by identifying, investigating, and remediating security threats and vulnerabilities. The Analyst is responsible for conducting forensic analysis, performing threat simulations, supporting incident response, and assessing cybersecurity risks. This role also involves recommending mitigation strategies and troubleshooting issues across various security platforms, including firewalls, identity and access management systems, and endpoint detection and response (EDR) tools.

Key Accountabilities and Expectations	
Key Accountability	**Expectation**
Strategy and Planning	• Contribute in the development to company-wide best practices for IT security and compliance • Contribute to the maintenance and enhancement of the enterprise's security awareness training program • Manage the annual updates of enterprise security documents (standards, baselines, guidelines and procedures)
Acquisition and Deployment	• Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors • Review security solutions or enhancements to existing security solutions to improve overall enterprise security • Participate in the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the enterprise's security documents specifically
Technology	• Maintain and implement technical security controls and processes in support of BC Transit's Information Security Management System • Monitor networks and systems for threats and potential security breaches • Investigate security incidents and other cybersecurity incidents • Collaborate with the Security Operations Center (SOC) to investigate and respond to security events of intermediate complexity • Configure and operate basic security software tools to safeguard systems and information infrastructure • Detect, assess, and mitigate vulnerabilities across networks, operating systems, web platforms, and on-premises applications • Support operating system and application patch management to ensure compliance with security standards • Support internal and external security audits and penetration testing activities • Provide end-user support for all deployed security solutions • Perform basic maintenance of secure baselines for all in-place systems and devices • Review and interpret logs and reports from security tools, identify anomalies, and recommend appropriate resolution • Provide basic security advice and support across all technology, including databases, servers, applications and cloud services

	• Monitor, review, and respond to security related IT service management tickets, escalating issues when necessary
Additional Duties	• Assists with conducting audits for security violations • Performs related duties in keeping with the purpose and accountabilities of the job

Summary of Qualifications and Job Specific Competencies	

Education	• University, college or technical degree/diploma in information technology.
	• Completion of two or more of the following certifications is considered an asset:
	  ○ Certified Information Systems Security Professional (CISSP)
	  ○ CompTIA CySA+
	  ○ ISC2 Systems Security Certified Practitioner (SSCP)
	  ○ Certified Ethical Hacker (CEH)
	  ○ ISACA Certified Information Systems Auditor (CISA)
	  ○ CompTIA Security+
	  ○ GIAC Certified Incident Handler (GCIH)

Experience	• Three (3) years related experience in managing enterprise level information security • Demonstrated expertise in applying security principles, with a solid theoretical foundation and hands-on experience in key cybersecurity areas such as multi-factor authentication (MFA), server patching, endpoint/server protection, and access management. • Proven ability to design and deliver engaging employee security awareness training programs • Experience managing IT service processes including configuration, change, and incident management, with a strong understanding of the Cybersecurity Incident Response Lifecycle • Familiar with cloud platforms such as Azure, particularly in relation to security, compliance, and risk mitigation • Working knowledge of security tools and practices including IDS/IPS, DLP, security event monitoring, vulnerability assessments, access control lists (ACLs), and digital forensics • An equivalent combination of education and experience may be considered
Key job-specific competencies	• Solid understanding of network segmentation, VLANs, and enterprise network architecture, with strong knowledge of TCP/IP and related network protocols • Strong knowledge of IT security best practices, frameworks (e.g., NIST, ISO), processes, and tools

	• Proficiency with Active Directory and Azure AD (Entra ID) configurations, and familiarity with major operating systems including Windows (client/server), Linux, and macOS • Demonstrated ability to prioritize and execute tasks effectively in high-pressure or time-sensitive environments • Strong investigative, analytical, and problem-solving abilities, with a detail-oriented approach • Excellent communication skills—both written and verbal—with the ability to convey technical information to non-technical audiences