SUNSHINE COAST REGIONAL DISTRICT **JOB DESCRIPTION**

INFORMATION TECHNOLOGY SECURITY ANALYST

EXEMPT (Y/N):	N	**DIVISION:**	Information Services
SALARY LEVEL:	Under Review	**DEPARTMENT:**	Corporate Services
LOCATION:	All	**SUPERVISOR:**	Manager, Information Services
APPROVED BY:	Manager, Information Services	**DATE:**	May 2023
Replaces:	*New*	*DATE:*	

SUMMARY

Under the general direction of the Manager, Information Services, delivers highly skilled security services including the development and administration of a comprehensive cyber security program, leads the development of plans and service implementations that balance security and information technology requirements while overseeing the SCRD's security infrastructure, monitors and improves security measures to protect the organization's networks, connected devices and information to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of the information or related systems.

KEY RESPONSIBILITIES *include:*

1. Plans, develops, implements, and delivers all services to ensure ongoing secure operation of the SCRD's information technology assets.
2. Provides ongoing assessment and evolution of security procedures for business continuity over networks, computer infrastructure, data assets, and end-user devices.
3. Develops and implements security policies, procedures, and incident response plans.
4. Communicates and trains staff on company-wide policies and best practices for IT security.
5. Develops and provides an ongoing training program for end-user security awareness.
6. Identifies weakness in security and continuously audits existing mitigation measures.
7. Conducts internal and external security audits, vulnerability testing, and risk tolerance analysis.
8. Designs, implements, maintains, and upgrades security systems, measures, policies, and controls.
9. Monitors networks and systems for cybersecurity attacks and data breaches.
10. Detects and investigates malicious activity to identify threat actors/vulnerabilities; and executes proactive mitigation strategies.
11. Investigates cyber incidents/breaches, gathers evidence, and executes prepared response plans.
12. Stays current on security methodologies, threat-landscape news, and cyber security organizations.

TYPICAL ACTIVITIES *include:*

1. Assesses current security risks and implement improvements.
2. Monitors networks and systems for security incidents and threat events.
3. Investigates incidents and responds to events in real time.
4. Writes detailed incident response report including root cause evidence and analysis.
5. Resolves vulnerabilities across all systems and networks.
6. Procures, configures, tests, installs, and maintains security software and hardware.
7. Develops and maintains best practice standards for information security.

8. Develops, implements, and maintains security protocols and procedures.
9. Conducts threat research through various information sources and cybersecurity partners.
10. Convenes and performs periodic risk assessments and penetration tests.
11. Defines appropriate access privileges to protect system processes.
12. Prepares and conducts user training and education communications.
13. Writes reports and provides consultation on the efficacy of security policies, incident responses, disaster recovery plans, business continuity plans, and other security-related information.
14. Develops detailed policies and procedures related to data protection, user activity monitoring, contingency planning, risk assessments, and incident response plans.

QUALIFICATIONS, EDUCATION, AND EXPERIENCE

- A bachelor's degree in computer science (or related field).
- A recognized designation in one or more of: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Risk and Information Systems Control (CRISC), or comparable.
- Total of 5 years' experience in the Information Technology/Information Security industry, with minimum of 2 years of experience as a Security Analyst or similar role, utilizing SIEM technologies.
- Valid BC Class 5 Driver's license.
- An equivalent combination of education and/or experience may be considered.

OTHER SKILLS/KNOWLEDGE/INFORMATION

- A thorough understanding of networking protocols, devices, intrusion detection/prevention, anti-virus software, log analysis tools, wireless access controls, and cloud computing technologies.
- Strong knowledge of pfSense firewall/router.
- Strong analytical skills with aptitude for recognizing threats and identifying risk mitigation strategies.
- Expert level IT skills including knowledge of networks, data centers, hardware, and software.
- Proficient use of scripting languages such as Python or JavaScript for automating security processes.
- Knowledge of operating systems (Windows, Linux) and virtualization platforms (VMware and Azure).
- Knowledge of encryption algorithms, cryptography, and cryptographic key management concepts.
- Proficient knowledge of Identity and Access Management solutions.
- Knowledge of cybersecurity best practices across wireless, mobile, and cloud networks.
- Thorough understanding of endpoint management.
- Ability to engage with all contacts with a customer-focused view and collaborative team approach.
- Ability to manage conflicting deadlines and handle multiple tasks successfully.
- Knowledge of applicable regulatory and legal requirements including software licensing, intellectual property rights, and data privacy legislation.
- Ability to maintain confidentiality where required and access/use data only in relation to job duties.