**SUNSHINE COAST REGIONAL DISTRICT** **JOB DESCRIPTION**

# CYBERSECURITY OFFICER

| | | | |
|---|---|---|---|
| **EXEMPT (Y/N):** | **Y** | **DIVISION:** | Information Services |
| **SALARY LEVEL:** | Exempt Level 4 (455 Points) | **DEPARTMENT:** | Corporate Services |
| **LOCATION**: | All | **SUPERVISOR:** | Manager, Information Services |
| **APPROVED BY:** | Manager, Information Services | **DATE:** | February 2024 |
| *Replaces:* | *New* | *DATE:* | |

**SUMMARY**

Under the general direction of the Manager, Information Services, this position is responsible for leading the development of a comprehensive cyber security framework and implementation of a defense-in-depth information technology (IT) security control program as well as providing work direction to the IT team, support to SCRD departments, and outreach to governance bodies to enhance security posture and to balance response to business continuity risks.

**KEY RESPONSIBILITIES** *include:*

1. Delivers highly skilled services including the development of standards and procedures of the IT security architecture, revision of disaster recovery plans, and oversight of the cybersecurity awareness program.
2. Monitors and improves security measures to protect networks, connected devices, and information from unauthorized access, use, disclosure, disruption, modification, or destruction.
3. Conducts highly sensitive internal and external security audits, vulnerability testing, and risk tolerance analysis.
4. Oversees the investigations of highly sensitive and extremely confidential cyber incidents/breaches, the thorough analysis, search and collection of relevant evidence, and the execution and updates to associated response plans.
5. Develops, leads, and oversees the SCRD's network and computer security posture.
6. Plans, implements, and delivers services to ensure secure operation of the SCRD's information technology assets.
7. Provides ongoing assessment and evolution of security procedures for business continuity over networks, computer infrastructure, data assets, and end-user devices.
8. Develops and provides an ongoing training program on company-wide policies and best practices for IT security and for end-user security awareness.
9. Identifies weakness in security and continuously audits existing mitigation measures.
10. Provides consultation on the adequacy of security policies, incident responses, disaster recovery plans, and business continuity plans.
11. Prepares and presents regular reports and updates to senior leadership on the status of the cyber security program, including key metrics, incidents, and trends.
12. Monitors networks and systems for cybersecurity attacks and data breaches.
13. Detects and investigates malicious activity to identify threat actors/vulnerabilities; and executes proactive mitigation strategies.
14. Stays current on security methodologies, threat-landscape news, and cyber security organizations.
15. Liaises with external partners, vendors, and regulatory agencies to ensure compliance with relevant laws, regulations, and industry standards.

**TYPICAL ACTIVITIES** *include:*

1. Assess current security risks and implement improvements.
2. Monitors networks and systems for security incidents and threat events.
3. Investigates security breaches, handles labour relations matters as necessary, 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 and implements appropriate access privileges to protect system processes.
12. Prepares and conducts user training and education communications.

**QUALIFICATIONS, EDUCATION, AND EXPERIENCE**

- A diploma in computer science or related field, bachelor's degree preferred.
- 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).
- Total of 5 years' experience in the Information Technology/Information Security industry, with minimum of 2 years in a cybersecurity delivery role, utilizing Security Information and Event Management (SIEM) technologies.
- An equivalent combination of education and/or experience may be considered.
- Valid BC Class 5 Driver's license.

**OTHER SKILLS/KNOWLEDGE/INFORMATION**

- Expert knowledge of cybersecurity best practices across wireless, mobile, and cloud networks, networking protocols, networks, data centers, hardware, software devices, intrusion detection/prevention, anti-virus software, log analysis tools, wireless access controls, and cloud computing technologies.
- Working knowledge of pfSense firewall/router.
- Proficient use of scripting languages such as Python or JavaScript for automating security processes.
- Proven ability to develop detailed policies and procedures related to data protection, user activity monitoring, contingency planning, risk assessments, and incident response plans.
- Strong analytical skills with aptitude for recognizing threats and identifying risk mitigation strategies.
- Working knowledge of operating systems (Windows, Linux) and virtualization platforms (VMware and Azure), encryption algorithms, cryptography, and cryptographic key management concepts, Identity and Access Management solutions.
- Working knowledge 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.