Comox Valley REGIONAL DISTRICT

Position Description

Position title: Cyber Security Manager	**Updated:** September 2025	**Job Family:** Professional/Technical 4
Reports to: Senior Manager of Information Systems and GIS	**Direct reports:** TBD	

POSITION SCOPE

The Cybersecurity Manager (Manager) plays a leadership role in ensuring the confidentiality, integrity and availability of the Comox Valley Regional District's (CVRD's) information and systems. This is a proactive and strategic role with emphasis on assessing, planning and implementing information security best practices. The Manager is directly responsible for delivering the IT security program for the organization, including related training, corporate awareness, policies, procedures, security breach investigations, and remedial action plans to ensure compliance with cybersecurity frameworks and security of all CVRD data. This position also has a lead role in compliance and risk management, assisting in the review of Privacy Impact Assessments to ensure compliance with the Freedom of Information and Protection of Privacy Act (FOIPPA).

KEY ACCOUNTABILITIES

1. Manages the development, implementation and delivery of the CVRD's Information Security Program.
2. Coordinates the development of security improvement initiatives.
3. In consultation with the Senior Manager, develops organization-wide Information Security policies and procedures.
4. Works with managers and staff across the organization to ensure that all CVRD staff remain adequately trained in best practices from a cybersecurity perspective.
5. Oversees and manages all corporate Firewalls, VPN appliances, security systems and security cameras.
6. Oversees and manages protection of Microsoft 365 with Microsoft Entra.
7. Oversees and manages all onboarding and offboarding of CVRD employees.
8. Maintains an awareness of current and emerging threats, completes risk assessments and directs appropriate responses.

9. Acts as a key resource and support to the CVRD's Chief Administrative Officer and local authorities on internal and external investigations involving security breaches and other IT policy contraventions.
10. Creates and tracks security metrics.
11. Stays current with security related technology and the changing threat landscape.
12. Works collaboratively within the Information Systems management team to establish and monitor the CVRD's cyber-security exposure, and changes in the threat landscape.
13. Participates in the development of business continuity planning; develops and sustains an information security incident response readiness and exercise function.
14. Collaborates with Engineering Services and other CVRD staff to define shared responsibilities around the secure and resilient operation of critical systems, identify needed improvements, and implement and monitor progress on these goals.
15. Conducts regular planning and preparedness exercises and events to ensure that the CVRD has the knowledge, ability, and plans to respond and recover from security threats.
16. Assists in the development of Privacy Impact Assessments as they relate to information and data security.
17. Leads and coordinates annual simulated cyber attack tests, or pen testing, on the organization's systems, networks, and applications to identify and exploit security vulnerabilities.
18. Responsible for identifying system weaknesses including user error and implementing remediation protocols to improve overall system security.
19. Responsible for setting the overall remote access security policy and thresholds for the organization and employees.
20. Responsible for overall data safety and security in both the implementation and ongoing support of payroll and HRIS legacy systems.
21. Mentors other Information Systems staff responsible for day-to-day security monitoring and response and the delivery of information security projects.
22. Manages vendors and consultants providing Information Security software, systems and services.
23. Provides guidance on the integration of information security practices to support service delivery and business case analysis as required for new and emerging corporate initiatives.
24. Directing and leading IT security personnel, including recruiting, training, performance management, and fostering continuous professional growth.

25. Establishes and maintains effective working relationships with internal and external stakeholders, including other business units, vendors, contractors, consultants, auditors, regulators, and various government agencies.
26. Manages the security budget and resources, ensuring optimal allocation and efficient utilization of funds and assets.
27. Acts as a liaison between industry peers, government agencies, and other specialists.
28. Prepares regular updates for EMT, boards, committees, and commissions, as required.
29. May be required to act in the place of the Senior Manager during extended absences.
30. May be required to participate in an activated Emergency Operations Centre.
31. Performs other duties as required.

QUALIFICATIONS

Education, Experience and Certification *(or equivalent combination where acceptable)*

- Undergraduate degree in Computer Science, Information Management or another related field.
- Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or equivalent.
- Minimum five years' recent related experience implementing and maintaining technology related to information security prevention, detection, and response
- Project management certification is preferred.

Knowledge, Abilities and Skills

- Considerable knowledge and understanding of the mandate, operating environment, business objectives, structure and operations of the regional district
- Strong knowledge of security systems configuration and operation technologies and practices including end-to-end problem management and root cause analysis.
- Knowledge of legal requirements for privacy of personal information from employees and local government including knowledge of the Province of British Columbia's *Freedom of Information and Protection of Privacy Act (FOIPPA)*
- Strong understanding of Microsoft Entra
- Ability to assess requirements and plan, develop, implement, maintain and support IT systems in a complex environment to facilitate achievement of business goals and objectives
- Ability to demonstrate a motivated approach to work including the ability to plan, prioritize and work under pressure, balance multiple demands and priorities to meet deadlines

- Ability to work in a team with diverse technical skills
- Ability to initiate and facilitate effective contacts with external consultants, vendors and service providers
- Ability to develop and deliver training and information sessions
- Ability to lead, coach and motivate staff in a team environment
- The ability to build and maintain strong partnerships with a variety of stakeholder groups and lead effectively toward a common goal
- Exceptional organizational and documentation capabilities
- Well-developed technical, analytical thinking and problem-solving abilities
- Skilled and experienced in risk management and risk assessment principles
- Strong awareness of confidentiality and discretion commensurate with the level of trust and access held by the position, which includes high level security access to all servers and security systems
- Strong organizational skills and the ability to perform effectively in high-stress incident response
- Excellent written and oral communication skills, especially when conveying technical information to diverse audiences.
- Well-developed consultative, facilitation, consensus building, conflict resolution and negotiation skills
- Strong stewardship of Comox Valley Regional District core values: collaboration, accountability, service, sustainability

EMPLOYEE SIGNATURE

This is to certify that I have read this job description:

_____	_____	_____
Print Name	Signature	Date