EMPLOYMENT OPPORTUNITY

Manager, Information Security

Permanent Full-Time | External
Information Services and GIS
Competition No.: 2026-1106

APPLICATION DETAILS

To apply for this position, send your cover letter and resume to **rdncareers@rdn.bc.ca,** clearly highlighting your education, experience, and qualifications relevant to the role. **Please quote 2026-1106 in the subject line of your email to ensure proper processing.**

Applications will be accepted until: 4:00 pm, on August 28, 2026.

Date Posted: August 7, 2026

We thank all applicants in advance for their interest; however, only those selected for further consideration will be contacted.

CRIMINAL RECORD CHECK

A satisfactory Criminal Record Check is a condition of employment with the Regional District of Nanaimo.

ABOUT THE ROLE

The Regional District of Nanaimo is seeking a permanent full-time **Manager, Information Security**, with the Information Services and GIS department. Reporting to the Chief Technology Officer, this position oversees the Regional District's Information Security Program, strengthening the resilience of the services our communities depend on every day. The role blends strategy, operational execution, team leadership, and relationship management. The Manager develops security plans, supports budget and resource planning, and uses current threat awareness to inform priorities. The position helps embed cybersecurity as a shared organizational responsibility, with meaningful work across security governance, vulnerability management, incident readiness and response, policy development, cyber awareness, security assessments, and resilience planning.

The successful candidate will bring sound judgment, clear communication, and practical leadership to turn plans and recommendations into action, building alignment across the organization and advancing security practices in ways that are achievable, measurable, and well understood.

QUALIFICATIONS

The role requires a minimum of eight (8) years of total experience in Information Technology or Security roles, including five (5) years implementing and maintaining information security technology for prevention, detection, and response, and three (3) years leading an Information Security practice, including program development, management, and staff supervision, ideally in a unionized environment.

Educational requirements include a degree in Computer Science or a related area, plus formal training and experience in information security resulting in a recognized credential equivalent to Certified Information Security Manager (CISM). A combination of equivalent education, skills, and experience may be considered.

A BC Class 5 Driver's License will be required.

POSITION DETAILS

This is a permanent full-time exempt position offering 35 hours per week with a salary range of $121,985 to $139,981 (2026 rate). This position offers a hybrid work arrangement and a competitive benefits package including the option to participate in the RDN's flex days program, and vacation entitlement that recognizes relevant previous experience.

www.rdn.bc.ca
rdncareers@rdn.bc.ca

POSITION TITLE: **Manager, Information Security**

REPORTS TO: **Chief Technology Officer**

DIRECT REPORTS: **Information Security Analyst (2)**

POSITION SUMMARY

The Manager, Information Security, plays a leadership role, responsible for advancing the Regional District of Nanaimo's Information Security Program and helping protect the systems, data, and services that support regional operations. Reporting to the Chief Technology Officer, this position translates cybersecurity risk into clear priorities, practical plans, and meaningful action across the organization. The role works with leaders, staff, vendors, and partner agencies to strengthen security practices, support appropriate resourcing, and embed security into corporate planning and service delivery. The Manager also supports compliance, risk management, privacy-linked security assessments, incident readiness, and continuous improvement of the RDN's security posture.

PRIMARY DUTIES AND RESPONSIBILITIES

- Manages the development and delivery of the RDN's Information Security Program.
- Manages, mentors and develops the Information Security team, which is responsible for day-to-day security monitoring and response and the delivery of information security projects.
- Coordinates the development of the Security Improvement and Sustainment Plan, supports the CTO in obtaining adoption of this plan, and leads the implementation of key initiatives.
- Plans, prioritizes, and develops budget in support of future year Information Security projects and services, and monitors current year expenditures, within the context of the overall Information Services and GIS Department budget.
- Drafts, collaborates on and, in conjunction with the CTO, obtains buy-in for organization-wide Information Security policies and procedures.
- Leads the RDN Cyber Awareness program, delivering education, managing simulation exercises, and working with managers across the organization to ensure that staff remain adequately trained in safe computing practices.
- Maintains an awareness of current and emerging threats through a combination of open-source research, relationships with peer local government leaders and senior government Information Security organizations, and the implementation of technology that provides continuous intelligence related to the RDN's security exposure.
- Works collaboratively within the Information Services and GIS management team to establish and monitor the Technology Vulnerability Management program.
- Collaborates with staff responsible for Operational Technology environments (e.g. Sanitary Sewer, Water, Solid Waste SCADA systems, Building Control Systems) and the Information Services and GIS management team to define shared responsibilities around the secure and resilient operation of critical systems, identify needed improvements, and implement and monitor progress on these goals.
- Participates in the development of business continuity planning; develops and sustains an information security incident response readiness and exercise function.
- Manages vendors and consultants providing Information Security software and services
- Prepares written reports for presentation at RDN Board and Committee meetings as required.
- May be required to attend Board or Committee meetings to present on Information Security initiatives
- Reviews, adheres to, and directs the adherence to safe work procedures in the workplace and generally promotes a safe work environment.
- May be required to act in the place of the CTO during absences.

- Performs other duties as required.

REQUIRED EDUCATION AND SKILLS:

- Four-year degree in Computer Science or a related area.
- Formal training and experience in information security resulting in a recognized credential equivalent to Certified Information Security Manager (CISM).
- Additional credentials in information security, project management, change management and information technology are highly desirable.

REQUIRED EXPERIENCE:

- Minimum eight (8) years of total experience in Information Technology or Security roles.
- Including five (5) years of experience implementing and maintaining technology related to information security prevention, detection, and response (e.g. EDR, email scanning, vulnerability management, firewall, SIEM / SOAR, IDS, IPS, security posture management, etc.).
- Including three (3) years of experience leading an Information Security practice, which must include program development, management and staff supervision, ideally in a unionized environment
- Combinations of equivalent education, skills and experience may be accepted.

SKILLS AND KNOWLEDGE:

- Proven leadership abilities, with strong interpersonal skills and ability to motivate staff.
- Proven ability to build relationships and influence individuals at all levels.
- Proficiency in program development, strategic planning, budgeting, and vendor management.
- Strong written and verbal communication skills.
- Strong awareness of confidentiality and discretion commensurate with the level of trust and access held by the position.
- Strong organizational skills and the ability to perform effectively in high-stress incident response.
- Strong ability to prioritize and manage multiple priorities with competing demands for resources.
- Strong analytical and problem-solving skills.
- Knowledge of IT end-to-end problem management and root cause analysis.
- Knowledge of the requirements of the *BC Freedom of Information and Protection of Privacy Act* related to Information Security.

This job requires travel to remote facilities, and by its nature, may involve exposure to sensitive personal and confidential information. As such, a Criminal Record Check, an enhanced employee confidentiality agreement and a BC Class 5 Driver's License will be required.