



# SECURITY ANALYST

---

**COMPETITION: #2267- 50040935**

**STATUS:** Regular full-time (Exempt)  
**SECTION:** Information & Communication Technology, Support Services  
**HOURS OF WORK:** Monday to Friday, 8:00 a.m. to 4:00 p.m. (35-hour work week)  
**SALARY:** Pay Range 90 - \$102,256 to \$127,830 annually  
**COMPETITION END DATE:** Friday, March 24, 2023

Responsible for planning and carrying out security measures to ensure the Department's infrastructures and digital assets are protected from unauthorized access, and detects and prevents cyber threats to the Department by identifying weaknesses in the environment and finding ways to protect the infrastructure.

## ESSENTIAL DUTIES

- Actively monitors the infrastructure for security issues, and prevents and stops unauthorized access; administers, monitors, and audits internet access and all security-related technologies, including remote user access systems
- Maintains and administers, or works with other team members, to ensure a secure implementation of Active Directory and group policies
- Plans, implements, administers, maintains, and monitors IT security controls for network, endpoint, server, application, etc.
- Performs vulnerability assessments to identify weaknesses and generate reports to evaluate the effectiveness of security measures
- Documents security issues, examines security breaches, gathers electronic evidence, and recommends and develops remedial actions
- Recommends and develops department-wide best practices for IT security; works with other team members to ensure the infrastructure is using sound architectural designs
- Coordinates any planning and participates in security audits, and risk and compliance assessments; participates in IT security investigations and cybersecurity exercise
- Researches and evaluates new and emerging IT security technologies and threats; works with other team members on designs, tests, and the implementation of security-related technologies, including developing business cases for security investments
- Provides periodic review, evaluation, and revision of existing policies to ensure their relevance and effectiveness; educates IT staff and other users on Departmental security policy and promotes general security awareness
- Other related duties and responsibilities as assigned

## KNOWLEDGE, SKILLS, AND ABILITIES

### Required:

- Ability to draw on knowledge and experience in different technology domains, combined with verbal and written communication skills, to convey complicated technical, security, and compliance concepts to peers and management
- Working knowledge of maintaining different security appliances, software, and systems monitoring tools
- Knowledge of network infrastructure, including routers, switches, firewalls, and the associated network protocols and concepts
- Knowledge of various cybersecurity technologies, architectures, and solutions
- Knowledge of managing digital certificates
- Knowledge and experience with information security policy frameworks (NIST 800-53, ITSG-33, etc.)
- Proficiency in performing risk, business impact, and vulnerability assessments
- Ability to establish and maintain effective working relationships in a team environment
- Excellent verbal and written communication skills
- Proven ability to organize work, exercise judgement, take initiative, and perform duties in an independent and confidential manner



- Strong leadership, analytical, and problem-solving skills
- Ability to deal effectively with staff at all levels of the organization

**Preferred:**

- Experience with blue-teaming, incident response, risk management, and designing network/security architectures

**EXPERIENCE**

**Required:**

- Minimum five years of IT security-related experience in managing government enterprise-wide security solutions

**Preferred:**

- Certified Information Systems Security Professional (CISSP), Certified Cloud Security Certification (CCSP), Certified Information Security Manager (CISM), and/or Certified Information Systems Auditor (CISA) certification(s) is highly desirable
- Prior working experience in military and/or law enforcement agencies is preferred

**EDUCATION**

**Required:**

- Diploma in computer science, MIS or related discipline

**Preferred:**

- Bachelor's degree in computer sciences, MIS or related discipline

**OTHER REQUIREMENTS**

- Valid BC Driver's licence
- All employees must maintain their enhanced security clearance while employed with the Vancouver Police Department, which will be renewed every five years or as required

**SELECTION PROCESS**

Selected candidates will be required to take a written test and must obtain a minimum 70% passing mark to move forward to the interview stage.

**NOTE: This position is exempt from the union.**

Applicants should submit a resume via email by 4:30 p.m. of the closing date. **The email should indicate clearly the competition number on the subject**, and made to the attention of Human Resources Section, via email [vpd.civilian.jobs@vpd.ca](mailto:vpd.civilian.jobs@vpd.ca).