

**TITLE:** Network and Security Analyst  
**SECTION:** Information Technology Department  
**REPORTS TO:** Director of Information Technology

---

#231

## **SUMMARY**

Reporting to the Director of Information Technology or designate, the Network and Security Analyst role is to ensure the delivery of IT services are meeting the needs of students, staff, schools and departments. The Network and Security Analyst also continuously develops improvement in instruction, learning and business practice. The Network and Security Analyst works closely with colleagues within IT and other departments, as well as with vendors, to take a lead department role in the areas of Network Services and Information Security.

---

## **DUTIES**

- Design, maintain and set standards for the District's enterprise network environment including switches, routers, firewalls, wireless and VoIP systems
- Serve as the internal escalation point on client and system network connectivity and performance issues, as well for incident handling response for information security incidents
- Develop and implement upgrade procedures and standards necessary to keep the network equipment at vendor and industry recommended levels
- Manage the life cycle of the district's network, wireless and network security infrastructure and work with departments to review ongoing needs for wireless, video surveillance, security access, building automation, and voice/video communications
- Create and maintain detailed documentation library for all areas of the network, including inventories, drawings, policies, standards and responses
- Develop, implement and operationalize network performance, utilization, incident and problem monitoring strategies and systems that lead to ongoing improvements in availability, capability, reliability, and security
- Research and track information about current security threats, potential vulnerabilities, and develop communication plans and/or programs to raise awareness amongst stakeholders, decision makers and our users
- Regularly assess the strength and risk levels of the District's security governance and current processes, and recommend, develop, monitor and analyze technical security controls and procedures to detect, report and remediate security incidents and risks
- Assist with security reviews and provide technical security guidance and advocacy in District projects involving the planning, design and/or architecture of new or existing internal, cloud, co-located IT infrastructure and vendor managed services
- Participate in change advisory board to review and evaluate planned technology changes in terms of information security risks

- Maintain a solid understanding of the K-12 learning environment, and the strategic and operational goals of the district
  - May, on occasion, be required to perform other related duties as assigned.
- 

## QUALIFICATIONS

- Bachelor's degree in Computer Science, Information Systems or related discipline
- 5+ years' experience in IT, including 2+ years' recent experience in a specialized Networking role and 2+ years in a specialized Information Security role
- 2+ years' design, implementation and support experience (Networking and Security context) with IaaS and PaaS infrastructure in cloud platforms such as Azure, AWS, etc.
- An equivalent combination of education and experience may be considered
- Industry certifications in networking, security, IT governance and ITSM:
  - Cisco CCNA/CCNP; Palo Alto PCNSA/PCNSE; (ISC)<sup>2</sup> SSCP/CISSP; ISACA CISA/COBIT; ITIL3+
- Data Centre experience in IT infrastructure support: Microsoft Server, VMWare, storage and DR.
- Knowledge, experience and training in IT governance, BCP/DR and BC privacy legislation
- Excellent written, verbal and interpersonal skills
- Excellent analytical skills and attention to detail
- Ability to collaborate effectively and work as part of a team, often in a lead role
- Experience and training in Project Management and Change Management methodologies
- Valid Class 5 BC Driver's License.