Job Description – IT Security Analyst	
Working Title:	IT Security Analyst
Department:	Information Technology
Manager/Supervisor:	Executive Director, Information Technology

Position Summary

Sooke School District is the fastest growing School District in British Columbia. Reporting to the Executive Director IT, the role of IT Security Analyst is responsible for performing skilled tasks under minimum supervision in providing infrastructure support and enhancements to the district's information technology systems. This role may be assigned to one or more projects, sometimes in a lead capacity, and/or operational work managing smaller changes in the technology environment. As a Senior role, this position lends ongoing coaching and mentoring support to team members.

Duties & Responsibilities

GENERAL

The IT Security Analyst plays a vital role in keeping the school district's digital assets, including proprietary and sensitive information secure and available. The security manager/analyst performs day-to-day operations of the in-place security solutions along with the identification, investigation, and resolution of security breaches. The Security Analyst assists the CIO in the implementation of new security solutions, participation in the creation and/or maintenance of policies, training, standards, baselines, guidelines, and procedures as well as conducting vulnerability audits and assessments to improve the overall security posture.

TYPICAL DUTIES

Leadership

- Lead the district in the implementation of Data Classification, Records Management and Security Solutions
- Create a security program roadmap and implementation
- Lead the design and execution of vulnerability assessments, penetration tests, and security audits
- Maintain current knowledge of the district risk tolerance and security goals as established by its stated policies, procedures, and guidelines and works actively towards upholding those goals
- Maintain up-to-date detailed knowledge of the IT security industry including new or revised security solutions, improved security processes, and the development of new attacks and threat vectors
- Create and coordinate awareness sessions to provide employees and other users with information on the use and application of required IT security protocols
- Contribute to and support the development, knowledge and application skills of IT staff with IT and cyber security techniques and processes
- Research, demonstrate and present in public, when directed by Supervisor, on current IT and cyber security issues and directions
- Assist the Chief Information Officer, IT Managers and relevant workplace leaders in providing recommendations related to privacy and the development of Privacy Impact Assessment (PIAs)
- Participate in the selection and analysis of all on-premise and cloud-based software solutions

- Promote and support the application of the Freedom of Information & Protection of Privacy Act (FIPPA) within the district. Respond to FOI requests as required.

Security Operations

- Maintain up-to-date baselines for the secure configuration and operations of all in-place devices, whether they be under direct control or not
- Maintain operational configurations of all in-house and cloud security solutions as per the established baselines
- Deploy, integrate, and complete initial configuration of all new security solutions and any enhancements to existing security solutions following standard best practices
- Perform regular assessments and audits of existing security systems, tools and controls
- Monitor all in-place security solutions for efficient and appropriate operations;
- Review and analyze logs and reports of all in-place and cloud services and devices and interpret the implications of that activity and devise plans for appropriate resolution
- Review and analyze metrics and data to filter out suspicious activity, and to find and mitigate risks before breaches occur
- Participate in, and may lead, investigations into problematic activity

Analysis and Planning

- Support and participate in the planning and design of enterprise security architecture, under the direction of the CIO, where appropriate
- Create and maintain enterprise security documents (policies, standards, baselines, guidelines, and procedures) under the direction of the CIO
- Generate reports for IT and district workplace leaders, as appropriate, and works with them to evaluate the efficacy of the security policies in place and assists in making necessary changes
- Contribute to the planning and design of an enterprise business continuity plan and disaster recovery plan
- Analyze, implement and administer electronic risk management profiles, including developing standards, protocols and data loss prevention recommendations.
- Participate in and analyze security risk assessments for 3rd party vendors, cloud solutions and software systems;
- Produce and communicate a Security Scorecard on a regular basis
- Experience working on all aspects of a managed project; design, implementation and support;
- Demonstrated a sound understanding of the Freedom of Information and Protection of Privacy Act (FIPPA)
- Demonstrated excellent “people” skills and effective communication
- Proven skills in developing operational documentation and written procedures
- Demonstrated ability to present ideas and strategies in language appropriate to varying audiences

Education/Experience:

- Bachelor's Degree in Computer Science, Business, MIS, Engineering or related field
- IT Certificates (Such as Microsoft and Apple Certified IT Professional) or equivalent experience/education
- One of the following security-related certifications: ISACA CISM or CISSP certification, GIAC Security Leadership Certification or equivalent
- ITIL Certification and Project Management certification a plus
- 7 years of technical experience in an Enterprise IT environment
- Knowledge of enterprise security standards including the CIS Critical Security Controls framework and ISO/IEC 27001
- Knowledge of formal security engineering methodologies and processes as described in NIST SP 800-160, COBIT or equivalent
- Knowledge of and experience working in a cloud environment with Agile and DevOps practices
- Six+ years of recent in-depth experience in day-to-day security-related operations
- Expert skills in Active Directory and Network architecture and administration
- Ability to remain current on malware protection, firewall protection, cloud computing, and other technologies
- Valid B.C. Class 5 Driver's license
- Track record of Technical Mentoring experience
- Business acumen in managing business relationships with internal and external stakeholders
- Exceptional communication skills (verbal and written),
- Analytical and problem-solving skills

COMPETENCIES:

Teamwork and cooperation is the ability to work cooperatively with diverse teams, workgroups and across the organization that includes the desire and ability to understand and respond effectively to other people from diverse backgrounds with diverse views.

Listening, Understanding and Responding is the desire and ability to understand and respond effectively to other people from diverse backgrounds. It includes the ability to understand accurately and respond effectively to both spoken and unspoken or partly expressed thoughts, feelings and concerns of others.

Organizational Awareness is the acumen to appreciate and the ability to use the power relationships in either one's own, or other, organization(s). This includes the ability to identify the real decision-makers and the individuals who can influence them, and to predict how new events or situations will affect individuals and groups within the organization.

Planning, Organizing and Coordinating involves proactively planning, establishing priorities and allocating resources. It is expressed by developing and implementing increasingly complex plans. It also involves monitoring and adjusting work to accomplish goals and deliver to the organization's mandate

Service Orientation implies a desire to identify and serve customers/clients, who may include the public, co-workers, other branches/divisions, other ministries/agencies, other government organizations, and non-government organizations. It means focusing one's efforts on discovering and meeting the needs of the customer/client.

Problem Solving/Sound Judgment is the ability to analyze problems systematically, organize information, and identify key factors and options leading to successful outcomes.