JOB DESCRIPTION
Puyallup School District
Exempt Level 6

Cyber Security Engineer Team Lead

Purpose Statement

The Cyber Security Engineer Team Lead is responsible to plan, design, implement and conduct the district's security strategy and recommend security enhancements to leadership with the goal of protecting personal/district data, computer systems and networks. This position is the process owner for cybersecurity incident management, plays an essential role on the Disaster Recovery team and shares responsibility for ensuring compliance with board policy 2022 (Electronic Resources and Internet Safety). The Cyber Security Engineer Team Lead should have a sense of urgency, be able to prioritize workload, communicate with professionalism and follow through to ensure that service levels are met and exceeded to meet the core mission of the district.

Essential Functions

- Works with department teams and various other departments to ensure coordination of team and resources to accomplish the needs and support of the district.
- Works with department staff and leadership to help plan, organize and align work priorities to meet and exceed service level objectives.
- Communicates proactively and clearly with various teams within the department and the district to ensure follow-through.
- Manages tasks, timelines, and deadlines with assurance to customers.
- Drives the success of the team and department constantly pushing the limits of what can be accomplished.
- Contributes knowledge and expertise of area to department leadership to help guide decision making.
- Maintains strict confidentiality of accessible district information resources.
- Assures network security, availability, and integrity.
- Collaborates with all department teams and leadership as well as other district staff, teams, and/or departments.
- Follows direction of department leadership.

Team Lead Focused Functions

- Helps develop short and long-range operational goals for Cyber Security Engineer team.
- Oversees technical documentation and procedures for individual and team use.
- Collaborates with department team leads and leadership around handling of sensitive matters helping to create procedures, train, and communicate to department staff to address future issues.
- Creates projects and work with members of Cyber Security Engineer team and other teams inside and outside of department for completing work.
- Fosters a collaborative culture, empowering others to succeed.
- Holds Cyber Security Engineers accountable for work being done and manages tasks, timelines, and deadlines with assurance to customers.
- Trains and helps Cyber Security Engineers in cyber security standards and procedures.
- Attends and leads meetings with other district departments to understand needs and coordinates work needed with department teams.
- Works with department leadership to periodically revise technology standards to best meet the needs of the district.
- Analyzes the critical nature of various requests and responds by adjusting resources and personnel as needed.
- Assists with cyber security tickets and requests submitted via ticketing system, phone calls, emails, messages, etc.
- Utilizes monitoring solutions for indications of compromise, issues, audit, anomalies, trends, and intrusions.
- Assists in performing forensic reviews using technology tools and log aggregators such as Public Records Requests, digital investigations, etc.
- Monitors, reviews, and collaborates with teams around patching of various systems and performing vulnerability scans.
- Develops policies, procedures, and playbooks for frequent security workflows (documentation) leveraging defense-in-depth methodology.
- Actively follows and engages with cyber security industry professionals' blogs, industry news, and forums of other cyber security professionals for latest strategies and emerging threats.
- Creates, analyzes, establishes, maintains, and updates security requirements for our systems/network.
- Actively defends network systems against unauthorized access, modification and/or destruction from both internal and external threats.
- Ensures that the district complies with statutory and regulatory requirements regarding information access, security, and privacy.
- Configures and support security tools such as Microsoft Defender ATP, Security and Compliance, etc.
- Trains fellow department staff in security awareness, policies, and procedures.
- Designs and conducts security audits to ensure operational security and make policy recommendations.
- Responds immediately to security incidents and provide post-incident analysis.

- Creates, updates, and maintains system and security documentation and configuration data for regulatory and audit purposes.
- Evaluates Cyber Security Engineers.
- Backs-up Cyber Security Engineers when needed to continue to meet service level expectations.

Other Functions

- Leads small teams to accomplish tasks, projects, and goals of department.
- Collaborates with department leadership to periodically revise technology standards to best meet the needs of the district's students and staff.
- Evaluates and responds to special requests for technology and/or support as will arise from time to time.
- Assists other personnel as may be required for the purpose of supporting them in the completion of their work activities.
- Attends meetings as assigned for the purpose of conveying and/or gathering information required to perform functions.

Job Requirements: Minimum Qualifications

Skills, Knowledge, and Abilities

SKILLS include analyzing and documenting existing security controls and review and update documentation; analyze security systems/controls and seek improvements on a continuous basis; evidence and chain-of-custody experience; an understanding of best practices and how to implement them at an enterprise level; help educate the workforce on common threats through cyber security training and awareness; critical thinking skills and the ability to solve problems as they arise; planning, researching and developing security policies, standards, and procedures; experience with scripting (PowerShell, Bash, Python, etc.); leading a team and others to ensure a clear understanding of the link between individual job assignments and the core mission and functions of the school district; setting and adjusting work priorities for a variety of technical support staff, reviewing, understanding, and communicating the importance of various data regarding ticket resolution and incident response; perform multiple tasks with the potential need to upgrade skills to meet changing job requirements.

KNOWLEDGE of different frameworks such as NIST SP-800 (or NIST CSF) and the MITRE ATT&CK Framework; disaster recovery strategies and incident response plans; computer forensic tools; the CIA Triad, what it means, and how to apply it using security controls; risk assessment/management tools, technologies, and methods; anti-virus software, intrusion detection, firewalls, content filtering; digital forensic tools.

ABILITY to lead others is required, including focusing on continuously improving the customer experience, working with various departments, groups, and people to ensure excellent customer service, and resolving conflicting priorities. Ability to communicate effectively with people at all levels of experience and responsibility throughout the district is required. Assist staff with computer operations and software problems; learn and develop new operations, procedures, processes and use of new equipment; articulate technical information to non-technical audiences in person, via written communication and telephone; organize, set priorities and work effectively under pressure; exercise sound judgement, including appropriate handling of confidential matters; learn continually and keep abreast of technological changes in the field; work independently with minimum supervision.

Responsibility

Responsibilities include, working under limited supervision following standardized practices and/or methods; providing information and/or advising others; and utilizing resources from other work units may be required to perform the job's functions. There is a continual opportunity to significantly impact the organization's services. Maintain regular and punctual attendance.

This position may require occasional work outside of normal business hours.

Working Environment

The usual and customary methods of performing the job's functions require the following physical demands: generally performed in an indoor office/school environment with frequent interruptions and noise associated with computer equipment, staff and students, and some exposure to risk of injury and/or illness; sitting/standing for prolonged periods; daily walking and moving between work areas; exposure to visual display terminal for prolonged periods; arm, wrist, elbow and hand movements associated with prolonged keyboarding; hand and finger dexterity.

Experience	Minimum five (5) years experience leading others in a supervisory role required. Minimum five (5) years experience of cyber security experience required. Minimum two (2) years experience planning, managing, prioritizing, assigning, and monitoring work to meet objectives of multiple or competing priorities/projects.
Education	Bachelor's degree in technology field or completion of equivalent training required. Holding one of the following professional certifications is preferred: CISSP, CISM, GSEC, CEH, Security+. Other experience and/or education may be substituted for required experience and/or education.

Required Testing

No pre-employment Proficiency Test is required

Valid Driver's License and Evidence of Insurability

Clearances

Criminal Justice Fingerprint/Background Clearance

Certificates/Licenses

None required