I.T. CYBER SECURITY

Purpose of Class

Performs a variety of Information Technology security duties relating to the monitoring, configuration, incident response and maintenance of Information Systems and security devices.

Primary Function

The IT Cyber Security Engineer's principal function is to work with the latest technologies to detect, analyze, and limit intrusions and security events. In addition, the IT Security Engineer will participate with the installation, monitoring, configuration, maintenance, support and optimization of all Information Systems and security devices. The individual will also establish and develop the Incident Response procedure and security training for district staff. The work is performed under the general supervision of the Technology Coordinator but considerable latitude is granted for the exercise of independent judgment and initiative.

Essential Duties and Responsibilities

- Develop and maintain Incident Response procedure
- Develop and maintain IT based security education and awareness programs for district staff
- Develop and ensure security policies, standards and guidelines
- Organize, implement and monitor security audit logs and access control practices to ensure adherence to policies and procedures
- Provide guidance on information security topics, advising and collaborating on security processes, business continuity and disaster recovery plans
- Perform security monitoring and incident response
- Ensure that system and application security design is in accordance with School District policy; consults with IT teams to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software
- Lead investigations of any actual or potential information security violations and manage escalation of security events; assist with related legal matters associated with such events as needed and make recommendations to correct or prevent future incidents
- Monitor external threat environment for emerging threats and advise relevant stakeholders on appropriate action
- Provide regular reporting on current state of information security program to the Technology Coordinator and other senior management
- Establish metrics and reporting framework to measure the efficiency, effectiveness and maturity of level of the program
- Liaise with relevant internal departments and external agencies as needed to ensure the School District maintains a strong security posture

- Work with Network Engineer and Application Specialists to audit, monitor and validate their environments security, including conducting gap analysis and other comprehensive internal assessments of existing systems to improve the security infrastructure and mitigate risks
- Provide oversight to the architecture and engineering of new security systems; including the evaluation of technical designs

Competency Requirements:

Knowledge of:

- Customer service skills and techniques
- Strong knowledge of common security management frameworks, such as ISO/IEC 27001, NIST and CSA.
- Strong knowledge of Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Children's Online Privacy Act (COPPA), Payment Card Industry Data Security Standard (PCI DSS) and Personally Identifiable Information (PII)
- Designing and managing new and existing security systems
- Contract and vendor negotiations

Ability to:

- Manage multiple, simultaneous security initiatives and responses
- Perform a high degree of initiative, dependability
- Advise district staff in securing their respective environments
- Exhibit strong written and verbal communications skills, interpersonal and collaborative skills
- Strong ability to convey security information to non-technical end-users in a way that inspires adoption and adherence to all IT and Board security policies and programs
- Establish priorities and work within time constraints and deadlines
- Audit security implementation access and violations against policies, procedures and regulations
- Perform diagnostics for complex multi-tasking security problems
- Communicate effectively and establish working relationships with users, other employees, administrators, and the public
- Perform multiple tasks simultaneously, including handling interruptions, and return to and complete tasks in a timely manner
- Work independently, with minimal supervision, and make appropriate decisions in the absence of a supervisor

Acceptable Experience and Training

- Associates Degree or Bachelors Degree in computer repair or related field
- Security certifications preferred
- Any equivalent combination of experience and training which provides the knowledge and abilities necessary to perform the work.

Essential Physical Abilities

- Sufficient clarity of speech and hearing or other communication capabilities, with or without reasonable accommodation, which permits the employee to discern verbal instructions and to communicate effectively in person and by telephone;
- Sufficient visual acuity, with or without reasonable accommodation, which permits the employee to comprehend written work instructions, comprehend technical manuals and diagrams, prepare written technical reports, troubleshoot and install and repair computer systems and equipment and organize documents and materials;
- Sufficient manual dexterity, with or without reasonable accommodation, which permits the employee to operate, install, maintain and make adjustments to computers and related equipment;
- Job tasks may require, with or without reasonable accommodation, sitting, standing, climbing, stooping, kneeling, crouching, reaching, standing, walking, lifting, grasping and repetitive motions.