SIERRA COLLEGE

Job Description

JOB TITLE: SECURITY SPECIALIST

PAY GRADE: CL 29

LAST REVISED: JUNE 2016

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job. Additional or different duties from the ones set forth below may be required to address changing business needs/practices.*

SUMMARY DESCRIPTION

Under the direction of a designated IIT supervisor, manager or Director, incumbents assigned to this classification ensure the secure operation of the in-house computer systems, servers, and network connections. This includes developing and identifying processes for checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting. The incumbent will also analyze and help resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user activity audits where required. Perform the process and provisioning of systems accounts with area leads. Maintain the security and provisioning of access to systems and related ancillary third party systems. Develop, conduct, and coordinate end user security training and information awareness.

REPRESENTATIVE DUTIES - *The following duties are typical for this job classification. Incumbents may not perform all of the listed duties and/or may be required to perform additional or different duties from those set forth below to address business needs and changing business practices.*

1. Ensures system and infrastructure security configurations system-wide are properly implemented and configured in conjunction with reducing the overall security risk to the District.
2. Stays current with advancements in technology relative to Technology security and related service configurations, alerts, and threats; makes recommendations to management on information security practices and procedures.
3. Evaluates new systems and products for security monitoring, responses, and implementation
4. Provides leadership, work direction, technical advice, and problem-solving assistance to act as a technical liaison with District security and technology committee(s) and campus staff in facilitating information security programs.
5. Performs and coordinates system security assessments, provides analysis to identify gaps in security configurations standards, best practices, and identifies and assures follow-up on necessary actions to correct information systems security issues.
6. Conducts testing of systems both internally and externally to ensure alignment of security practices, goals, and assists in the prevention and mitigation of threats.
7. Designs, performs, and/or oversees security testing of all systems in order to identify system vulnerabilities including incident response processes and procedures.
8. Performs and implements processes in efforts to educate and inform staff, faculty, and students as to security best practices, awareness, and procedures.
9. Contributes technical expertise to district security procedures by working with the District's IIT management, technical staff, and information security teams or committees to assure a comprehensive District information systems and infrastructure security program.

10. Designs, implements, and administers access security and permissions for use of District-wide systems; establishes and enforces District systems access rules, standards and protocols.
11. Participates in and makes recommendations for backup and recovery procedures.
12. Develops and documents procedures to assist help desk and other staff in operating systems security; creates rules for use with security best practices.
13. Develops and maintains a Security Incident Response Plan for the District in collaboration with technical committees, security teams, functional leads, and IIT staff, and assures the plan is periodically tested and updated.
14. Researches and design's security counter measures while keeping current on technology security issues and procedures.
15. Monitors wired and wireless network traffic and implements approaches that optimize network security.
16. Assures overall operability of the District's Identity Management process and systems by coordinating with both functional and technical staff.
17. Reviews user roles and account access privileges and monitors accounts, password processes, and permissions to include account provisioning processes. This may include security access to databases, monitoring database access, file systems and reviewing policies and procedures.
18. Assures Change Management procedures are in compliance with system changes related to security prevention and correction.
19. Participates in regular Technical Support meetings to ensure customer concerns are discussed.
20. May train and provide work direction to assigned student workers and temporary help as assigned.
21. May require travel between sites compensated per diem based on district mileage reimbursement policy. May require on-call and weekend duties.
22. Performs related duties as required.

QUALIFICATIONS - *The following generally describes the knowledge and ability required to enter the job and/or be learned within a short period of time in order to successfully perform the assigned duties.*

Knowledge of:

Information systems security concepts, methodologies, analysis, and design to include best practices.
Systems planning, security principles, and general application management best practices
Current Windows network operating systems including installation, security, upgrading, and troubleshooting.
Single sign-on and lightweight directory access protocols, including Kerberos and CAS authentication protocols.
Language and writing skill to read, understand, and prepare system documentation and instructions.
Testing, flowcharting, and data mapping tools and procedures.
Data privacy practices and laws
Math skills to record sums, fractions, and statistical data.
Interpersonal skill to convey technical concepts to others and to facilitate problem solving with individuals and small groups.

Ability to:

Conduct research into security issues and products as required.

Analyze, conceptualize, and problem solve.
Understand the District's goals and objectives.
Work independently and collaboratively, follow logical progressions of systems and think logically, creatively, and in abstract terms.
Adapt to changing technologies and learn functionality of new equipment and systems.
Read and interpret technical manuals and other documentation.
Communicate clearly, collaboratively, and concisely, both orally and in writing.
Establish and maintain effective working relationships with those contacted in the course of work.

Education and Experience Guidelines: *Any combination of education and experience that would likely provide the required knowledge and abilities is qualifying. A typical way to obtain the knowledge and abilities would be:*

Education/Training:

Bachelor's degree from an accredited college or university with major course work in mathematics, data systems, computer science, or a related field, supplemented by specialized training in applications, enterprise systems management or systems analysis.

Experience:

Four years of increasingly responsible experience in the the security industry or closely related field. Industry certifications or experience may substitute for some higher education. Experience with corrective controls that serve to protect information resources; computer security issues, requirements and trends; information security standards and laws, including HIPAA and FERPA, etc.; current technologies and best practices methodologies including auditing or evaluating security systems and the services available to assess the security of information systems and data network transport systems.

License or Certificate:

Possession of a valid California driver's license.

One or more of the following certifications is desired (these are examples as others may be considered):

a) CISM: Certified Information Security Manager
b) SSCP: Systems Security Certified Practitioner
c) SANS/GIAC: Global Information Assurance Certification
d) CISSP: Certified Information System Security Professional
e) CISA: Certified Information Systems Auditor

PHYSICAL DEMANDS AND WORKING ENVIRONMENT - *The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential job functions.*

Environment: Work is performed primarily in a standard office setting.

Physical: Primary functions require sufficient physical ability and mobility to work in an office setting; to stand or sit for prolonged periods of time; to occasionally walk, stoop, bend, kneel, crouch, reach, and twist; to lift, carry, push, and/or pull light to moderate amounts (25 pounds) of weight; to operate office equipment requiring repetitive hand movement and fine coordination including use of a computer keyboard; and to verbally communicate to exchange information.

Vision: See in the normal visual range with or without correction.

Hearing: Hear in the normal audio range with or without correction.