SIERRA COLLEGE

Job Description

JOB TITLE: Security Specialist - ITS

PAY GRADE: CL 30

LAST REVISED: July 2025

*Job Descriptions/Class Specifications are intended to present a descriptive list of the range of duties performed by employees in the job and are **not** intended to reflect all duties performed within the job.*

Sierra College has a strong commitment to the achievement of equity and inclusion among its faculty, staff, and students and values the rich, diverse backgrounds that make up the campus community. A strong candidate for this position must have the understanding and ability to successfully support individuals with varying backgrounds. This includes persons with disabilities, various gender identities and sexual orientations, as well as individuals from historically underrepresented communities and other groups. Our District is committed to providing strategies for success and proactive student-centered practices and policies focused on eliminating equity gaps to ensure the District provides an inclusive educational and employment environment focused on strategies for success and equitable outcomes for all.

SUMMARY DESCRIPTION

Under general supervision from assigned manager, ensures the secure operation of District computer systems, servers, and network connections, including developing and identifying processes for checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting issues; analyzes and helps to resolve security breaches and vulnerability issues; performs the processing and provisioning of systems accounts with area leads; maintains the security and provisioning of access to systems and related ancillary third-party systems; develops, conducts, and coordinates end user security training and information awareness.

REPRESENTATIVE DUTIES

The following duties are typical for this 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. Stays current with advancements in technology security and related service configurations, alerts, and threats; makes recommendations to management on information security practices and procedures; researches and designs security counter measures; evaluates new systems and products for security monitoring, responses, and implementation.
2. Ensures system and infrastructure security configurations are implemented and configured in conjunction with reducing security risks to the District; designs, implements, and administers access security and permissions for use of District systems; establishes and enforces District systems access rules, standards, and protocols; ensures change management procedures comply with security prevention and correction system changes; monitors wired and wireless network traffic; implements approaches that optimize network security; reviews and monitors user roles, accounts, access privileges, password processes, and permissions, including account provisioning processes and security access to databases, monitoring database access, file systems and reviewing policies and procedures.
3. Serves as a technical liaison for District security and technology committees and District staff, including providing leadership, work direction, technical advice, problem-solving assistance, and information on security programs; contributes technical expertise for District security procedures.
4. Performs and coordinates system security assessments; designs, performs, and oversees internal and external security testing of District systems to identify vulnerabilities, including incident response processes and procedures; assists in the prevention and mitigation of threats; provides analysis to identify gaps in security configurations standards, and best practices; identifies and ensures follow-up on actions to correct information systems security issues.
5. Performs and implements processes to educate and inform District staff and students of security best practices, awareness, and procedures.
6. Participates in and makes recommendations for backup and recovery procedures.

7. Develops and maintains the District Security Incident Response Plan in collaboration with technical committees, security teams, functional leads, and ITS staff; ensures the plan is periodically tested and updated.
8. Develops and documents procedures to assist service desk and other staff in operating systems security; creates rules for use with security best practices.
9. May provide onboarding support, general work training, guidance, supervision assistance, and directs activities of students or temporary employees.
10. Performs related duties that support the overall objective of the position.

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:

- Security concepts, methodologies, analysis, design, and best practices of information systems, including systems planning, security principles, vulnerability and exploit assessment, and general application management.
- Penetration testing and knowledge of ethical hacking tools.
- Windows network operating systems, including installation, security, upgrading, and troubleshooting.
- Single sign on and lightweight directory access protocols, including Kerberos and Certificate of Advanced Studies (CAS) authentication protocols.
- Testing, flowcharting, and data mapping tools and procedures.
- Federal, state, and local laws, codes, and regulations regarding information technology and systems security, including, but not limited to, data privacy, the Family Educational Rights and Privacy Act (FERPA), and Health Insurance Portability and Accountability Act (HIPAA).
- Basic mathematical concepts.
- English usage, grammar, spelling, punctuation, and vocabulary.

Ability to:

- Oversee and participate in the management of a comprehensive software analysis program, including systems analysis, design, development, and implementation.
- Understand security vulnerabilities and attack vectors to safeguard District assets.
- Lead security analysts and technical staff in finding and remediating security threats.
- Conduct research into security issues and products.
- Analyze, conceptualize, and problem solve.
- Follow logical progressions of systems and think logically, creatively, and in abstract terms.
- Read, understand, and prepare system documentation and instructions.
- Read and interpret technical manuals and other documentation.
- Adapt to changing technologies and learn functionality of new equipment and systems.
- Maintain a high level of attention to detail.
- Implement countermeasures with minimal business impact.
- Convey technical concepts to others.
- Plan and organize work to meet schedules and changing deadlines.
- Perform basic record keeping functions.
- Utilize office procedures, methods, and equipment, including computers, technology, and applicable software applications sufficiently to perform the duties of the classification, including those used in technology security and management.
- Maintain confidentiality of information.

- Perform arithmetic calculations of average difficulty.
- Follow oral and written directions.
- Communicate clearly and concisely, both orally and in writing.
- Provide onboarding support, general work training, guidance, supervision assistance, and direct activities of students or temporary employees.
- Establish and maintain effective working relationships with those contacted in the course of work.
- Coordinate with staff and others to minimize delays or interruptions to District activities.
- Respond to emergencies.
- Work independently and collaboratively.
- Apply District policies and procedures.

EDUCATION AND EXPERIENCE GUIDELINES

Any combination of education and experience that demonstrates the required above knowledge and abilities is qualifying. Examples of ways to obtain the above knowledge and abilities could include, but are not limited to, the following:

Education/Training

- Two years of college with major course work in data systems, computer science, cyber security, or a related field, supplemented by specialized training in applications, enterprise systems management, or systems analysis.
- Industry certifications in cybersecurity may substitute for some education.

Experience

- Four years of increasingly responsible experience in the cyber security industry or closely related field.

License/Certificate - *Possession of, or ability to obtain within a reasonable timeframe, each of the following:*

- Valid California Driver's License.
- One or more of the following certifications is desired, although others may be considered:
  - Certified Information Security Manager Professional (CISM).
  - Systems Security Certified Practitioner (SCCP).
  - Global Information Assurance Certification (SANS/GIAC).
  - Certified Information System Security (CISSP).
  - Certified Information Systems Auditor (CISA).

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; may travel from site to site. Position may be required to work evenings, nights, and weekends.

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 of weight up to 25 pounds; 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.

Board Approved: July 15, 2025