DIRECTOR, SECURITY AND INFRASTRUCTURE SYSTEMS

Reports to:	Associate Vice President / Chief Information Systems Officer		
Dept:	Information Technology Services	**Range:**	CM-17
FLSA:	Exempt	**EEO:**	Executive/Administrative/ Managerial

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 by individual positions.

BASIC FUNCTION:

Under general direction, manages the security and infrastructure team, provides strategic leadership and guidance for the architecture, development, implementation, integration, maintenance, and enhancement of the district's information security and infrastructure systems; network security systems, processes, and policies; architects and implements the district's cloud-first strategy; manages budgets; oversees all data center system administration activities including cloud services, systems, servers, and network devices; and perform related duties as assigned.

ESSENTIAL DUTIES & RESPONSIBILITIES:

The duties listed below are intended only as illustrations of the various types of work that may be performed. The omission of specific statements of duties does not exclude them from the position if the work is similar, related or a logical assignment to this class.

Supervisory Responsibilities

1. Recruits, interviews, recommend hires, and trains staff.
2. Oversees scheduling, assignments, and the daily workflow of the department.
3. Provides constructive and timely performance evaluations.

Duties/Responsibilities

4. Exhibit an equity-minded focus, responsiveness, and sensitivity to and understanding of the diverse academic, socioeconomic, cultural, gender identity, sexual orientation, and ethnic backgrounds of community college students, and employees, including those with physical or learning disabilities, and successfully foster and support an inclusive educational and employment environment.
5. Plan, organize, schedule, and manage security upgrades on critical IT infrastructure; update the district's security plan, incident response plan, business continuity plan, and respond to any cyber incidents or events that occur.

6. Ensure appropriate security policies, NIST and CIS controls are applied to all workstations, devices, infrastructure, and server systems; perform routine security audits and oversee mitigation efforts; serve as the IT security officer and main point of contact for law enforcement and/or other authorities in the event of a cybersecurity incident.

7. Create, implement, and update security related policies, procedures, protocols, and practices to meet current requirements; assist in the communication and reporting of the district's cybersecurity stance, support, and resources as needed.

8. Assist in the secure management and maintenance of the district's network authentication systems, technology infrastructure, and security systems, including but not limited to, enterprise systems, servers, firewalls, backup, network, physical plant, data centers, disaster recovery systems, email security, and office suite environment; manage and maintain the district's security event information system and data loss prevention software.

9. Design, plan, test, implement, and document complex security enhancements and refresh cycles to the network infrastructure; manage and track budgets; oversee all outsourced managed detection and response or security operations; determine program needs, budget requirements, and ensure maximum return on investment.

10. Coordinate security related projects and work activities between technical operations, enterprise applications, and network systems staff; architect, implement, and support the district's cloud first strategy.

11. Implement system software/hardware security standards, upgrade procedures, and maintenance activities to meet reliability, security, accessibility standards, and expectations; troubleshoot network hardware and operating problems, including but not limited to connectivity, cloud services, internet access, e-mail, and servers;

12. Develop and maintain complete and accurate records pertaining to hardware, software, system, and network configurations, changes, outages, and improvement plans; direct data compilation and perform analysis as directed.

13. Recommend new technologies and/or upgrades to current technologies to improve security; promote and coordinate the development of training and education on IT security and related matters; develop appropriate security incident notification procedures.

OTHER DUTIES:

1. Represents the department on committees and workgroups and attends meetings related to district's the selection, implementation and use of computing facilities and resources.

2. Represent the district effectively in dealings with vendors, other community colleges and industry groups; attend related meetings and workshops.

3. Monitor and review new technology products and technology tools; review available information in industry publications, technical websites and others to evaluate opportunities to better meet district business, operational, productivity and technical requirements.

4. Maintains up-to-date technical knowledge by attending educational workshops, conferences, trainings, reviewing professional publications, establishing personal networks and

participating in professional associations to keep up with the industry regarding the district's IT portfolio, mission, and vision.

5. Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

1. Methods and procedures of standardizing, securing, maintaining, and operating computers and peripheral equipment in an enterprise environment.
2. Software License compliance laws and methodologies.
3. Cloud services as it relates to security and infrastructure systems.
4. Current server virtualization, network switching and routing, firewalls, data backup and recovery solutions, cloud computing resources, VoIP systems, business software applications (e.g. Office 365), and related systems used by the district.
5. Security and business continuity, disaster recovery and backup planning and execution.
6. Troubleshooting, diagnostic techniques, procedures, equipment and tools used in computer and peripheral repair.
7. Principles and practices of public budget management, purchasing and maintaining public records.
8. Technology documentation and presentation techniques.
9. Project management methods and techniques.
10. Professional and effective oral and written communication at all times.
11. Principles, practices and methods of network architecture, cyber-security infrastructure, and vulnerability management.
12. Principles and methods of enterprise-level data management and data storage technology solutions.
13. Research methods and analysis techniques including cost-benefit analyses.
14. District human resources policies and labor contract provisions.
15. Safety policies and safe work practices applicable to the work.

ABILITY TO:

1. Apply current NIST and CISO standards to current operations, and respond to security incidents and events.

2. Plan, organize, manage, assign, delegate, review and evaluate the work of staff engaged in providing information technology security and infrastructure services to the district and community.
3. Delegate, plan, schedule and perform complex maintenance and upgrades to all infrastructure located both on-premises and in the cloud.
4. Establish and maintain effective and cooperative working relationships by exhibiting courtesy, tact, patience, and diplomacy.
5. Effectively collaborate with other Information Technology Services (ITS) teams and departments to optimize results.
6. Communicate effectively and clearly both verbally and in writing, including logical and persuasive proposals, comprehensive correspondence, reports, studies and other written material.
7. Maintain current knowledge of technical advances in all areas of responsibility.
8. Analyze networking systems to modify current standards and develop innovative solutions to address changing conditions.
9. Understand and apply functional requirements to the development of systems proposals, specifications and recommendations for cost-effective information systems and technology solutions.
10. Develop and implement appropriate procedures and controls.
11. Understand, interpret, explain and apply applicable laws, codes and ordinances.
12. Deliver first-class customer service; assess customer needs, set priorities and allocate resources to most effectively meet needs in a timely manner.

EDUCATION AND EXPERIENCE:

Bachelor's degree from an accredited institution in information security, electrical engineering, electronics engineering, information technology, computer science, cybersecurity, or other related field and five (5) years of progressively responsible experience in information security and/or infrastructure systems in support of a complex enterprise level network; or an equivalent combination of training and experience.

LICENSES AND OTHER REQUIREMENTS:

A valid California driver’s license and the ability to maintain insurability under the district’s vehicle insurance program.

DESIRED QUALIFICATIONS

License or Certificate
SSCP - Systems Security Certified Practitioner and/or
CISSP - Certified Information Systems Security Professional

WORK DIRECTION, LEAD AND SUPERVISORY RESPONSIBILITIES:

Assigned classified staff, student and temporary workers, cloud service providers, vendors/contractors, and other staff as assigned.

CONTACTS:

Administrators, faculty, staff, students, network service providers, vendors and other community college IT managers and staff.

PHYSICAL EFFORT:

The physical efforts described here are representative of those that must be met by employees to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Primarily sedentary with intermittent standing, walking, bending and stooping; occasional light lifting and carrying of objects weighing up to 25 pounds; ability to travel to a variety of locations on and off campus as needed to conduct district business.

EMOTIONAL EFFORT:

Ability to develop and maintain effective working relationships involving interactions and communications personally, by phone and in writing with a variety of individuals and/or groups from diverse backgrounds on a regular, ongoing basis; ability to work effectively under pressure on a variety of tasks concurrently while meeting established deadlines and changing priorities.

WORKING CONDITIONS:

Primarily business office environment; subject to frequent public contact and interruption; intermittent exposure to individuals acting in a disagreeable fashion; may work at any district location or authorized facility with occasional evenings, weekends, and/or holidays on an as-needed basis. Occasional local travel may be requested.