Security Manager, Information Technology

BASIC FUNCTION

Under general direction of assigned supervisor, manages assigned personnel, provides strategic leadership and guidance for the architecture, development, implementation, integration, maintenance, and enhancement of the district's information security systems; network security systems, processes, and policies; architects and implements the district's cloud security strategy.

DISTINGUISHING CHARACTERISTICS

Incumbents in this position are 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 travel may be requested.

ESSENTIAL DUTIES & RESPONSIBILITIES

The following duties and responsibilities described below are intended only as illustrations of the diverse 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.

1. Personnel staffing, supervision, evaluation, and training/professional development.
2. Oversees scheduling, assignments, and the daily workflow of assigned staff (classified staff, student and temporary workers, cloud security service providers, security vendors/contractors, and other staff as assigned).
3. 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.
4. Plan, organize, schedule, and manage security upgrades on critical IT (Information Technology) infrastructure; update the district's security plan, incident response plan, business continuity plan, and respond to any cyber incidents or events that occur.
5. Ensure appropriate security policies, NIST and CIS (Center for Internet Security) controls are applied to all workstations, devices, infrastructure, and server systems; perform routine security audits and oversee mitigation efforts.

6. 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.

7. As it relates to cyber security 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.

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

9. Coordinate security related projects and work activities between technical operations, enterprise applications, and network systems staff.

10. Implement system software/hardware security standards, upgrade procedures, and maintenance activities to meet reliability, security, accessibility standards, and expectations.

11. Recommend innovative 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 innovative technology products and technology tools; review available informa-tion 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.

QUALIFICATIONS

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.

Skills and Abilities To:

1. Apply current NIST standards and CIS controls 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 meet needs most effectively 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 three (3) 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.

Certificates, Licenses, Special 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

Other Requirements:

Imperial Community College is committed to creating an academic and work environment that fosters diversity, equity, and inclusion and equal opportunity for all, and ensures that students, faculty, management, and staff of all backgrounds feel welcome, included, supported, and safe. Our culture of belonging, openness, and inclusion makes our district a unique and special place for individuals of all backgrounds. It is important that our employees' values align with our District's mission and goals for Equal Opportunity, Diversity, Equity, Inclusion, and Access.

WORKING CONDITIONS

Work Environment:

Office.

Physical Demands:

Work is performed primarily in a standard office environment with frequent interruptions and distractions; extended periods of time of viewing a computer monitor.

Requires sufficient physical ability to work in an office setting; to stand or sit for prolonged periods of time; to occasionally stoop, bend, kneel, crouch, reach, and twist; to lift, carry, push, and/or pull light to moderate amounts of weight; to operate office equipment requiring repetitive hand movement and fine coordination including use of a computer keyboard; 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.

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions of this classification.

Mental Demands:
Work in an environment of frequent interruptions and possible dissatisfied individuals.