



Director, Security and User Services

Management Range: 19

Board Approved: 06/08/2023

P. 1|4

*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; however, any additional duties will be reasonably related to this class.*

SUMMARY DESCRIPTION

Under the direction of the appropriate administrator, provides leadership for all aspects of Information Security and User Services. In addition, this position will support the implementation of District Strategic and Tactical Technology Plans.

REPRESENTATIVE DUTIES

The following duties are typical for this classification.

1. Responsible for the planning and prioritization of District security projects and tracking the progress of security initiatives.
2. Ensures that the District's IT security practices adhere to relevant legal, regulatory, and compliance requirements, such as the Family Educational Rights and Privacy Act (FERPA), and Health Insurance Portability and Accountability Act (HIPAA) if applicable.
3. Leads and facilitates risk assessments, network audits, and internal auditing.
4. Develops and implements comprehensive cybersecurity policies and procedures to protect the District IT infrastructure and data.
5. Conducts regular vulnerability and risk assessments, penetration testing to identify and mitigate security risks.
6. Develops and implements disaster recovery and business continuity plans to ensure the District's IT infrastructure can withstand potential disruptions.
7. Collaborates with other areas, such as administration and human resources to ensure that security measures are integrated into various processes and initiatives; coordinates with external partners, such as cybersecurity vendors as necessary.
8. Develops, implements, and manages District-wide IT security incident response processes and procedures.
9. Develops and implements strategies for complying with applicable Federal, State and other legal compliance requirements related to IT Security.
10. Develops, implements, and manages a District-wide IT security awareness and training program including designing and delivering security awareness programs and training sessions to educate faculty, staff, and students about safe computing practices, data protection, and cybersecurity threats.
11. Stays updated with the latest IT security trends, threats, and technologies by conducting research, attending conferences, participating in professional development activities, and continuously improving the District's IT security posture.
12. Provides leadership and oversight for the delivery of effective Help Desk Services for students, faculty, and staff throughout the District.
13. Sets, tracks, measures, and reports on key support performance metrics for Help Desk Services.



Director, Security and User Services

Management Range: 19

Board Approved: 06/08/2023

P. 2|4

14. Promotes customer focused support and implements continuous improvements to support services to improve the accountability of service delivery.
15. In coordination with campus technology leadership, establishes, communicates, and monitors IT support service level agreements (SLAs).
16. Coordinates, develops, and implements Asset Management processes and procedures for IT hardware and software.
17. Establishes and manages procedures to ensure effective support coordination between IT Help Desk Services (Tier 1), Tier 2 and Tier 3 resources.
18. Manages Desktop Support services for SBCCD's District Office location; assists in managing and prioritizing incoming service requests; gathers and analyzes Help Desk metrics and performance data to generate reports and identify trends.
19. Stays updated with emerging technologies and trends relevant to Help Desk operations; evaluates new tools and solutions to enhance the Help Desk's efficiency and effectiveness.
20. Provides leadership, direction, and coaching to assigned staff to assure current and continuing competencies in the fields necessary for effective performance.
21. Performs related duties as required.

MINIMUM 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:

- An effective IT security system and network architectures, concepts, techniques and tools.
- Principles and practices of managing network and system security system security components such as firewalls and intrusion detection/prevention systems.
- IT security management, industry best practices and standards
- Principles and practices of developing and implementing IT security policies and procedures.
- Technology areas such as applications, systems and networks and the inter-relationships between them.
- Service desk tools and best practices
- How information technology is used in instruction and college support programs.
- Principles and practices of administration, supervision, training and performance evaluation.
- Principles and practices of budget preparation and administration.
- Characteristics and capabilities of modern technological equipment; telecommunications systems, operations and development.
- Principles and practices of program development administration.

Ability to:

- Identify, analyze, prioritize and communicate impact of IT security risks and exposures.
- Develop cooperative working relationships in a highly diverse environment.
- Manage a complex information technology organization.



Director, Security and User Services

Management Range: 19

Board Approved: 06/08/2023

P. 3|4

- Communicate effectively both orally and in writing.
- Develop and administer policies and procedures.
- Oversee, direct, and coordinate the work of lower-level staff.
- Gather and analyze data and situations and make appropriate decisions.
- Prepare and present comprehensive, concise, clear oral and written reports.
- Analyze problems, identify alternative solutions, project consequences of proposed actions and implement recommendations in support of goals.
- Interpret and apply California Education Code, Title 5, federal, state, and local policies, laws and regulations as it relates to the position.
- Demonstrate professionalism, fairness and honesty in all aspects of the performance of duties.
- Provide leadership based on ethics and principles as they relate to campus technology functions and operations.

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:

- A Bachelor's degree from an accredited college or university in a related field.

Required Experience:

- Four (4) years of experience in IT Networks, Systems or Security related positions.
- Experience that indicates a sensitivity to and understanding of the diverse socioeconomic, cultural and ethnic backgrounds of staff and community college students and staff to staff and students with physical and learning disabilities.

Preferred Education/Experience:

- Certifications such as CISSP (Certified Information System Security Professional), CISM (ISACA Certified Information Security Manager) or CISA (ISACA Certified Information Security Auditor).
- Experience in the California Community College System.

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 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.



Director, Security and User Services

Management Range: 19

Board Approved: 06/08/2023

P. 4|4

Vision: See in the normal visual range with or without correction; vision sufficient to read computer screens and printed documents; and to operate assigned equipment.

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