

Job Description



Position Title: IT Security Compliance Administrator

Department: Technology Services

Employment Category: Exempt Staff

Primary Location: District-wide
Based on the Sierra Vista Campus

FLSA Classification: Exempt
Remote Work Eligible: No

Parameters: Full-Time; 12 Months/Year

Pay Grade: EX11

Position Summary: The IT Security Compliance Administrator is responsible for verifying the District operates in accordance with its information security policies and related procedures and technical controls, including all processes and standards related to inventory management, configuration management, patch management, vulnerability management, third party security due-diligence, disaster recovery, business continuity, and security incident response and for performing the District's Identity and Access Management procedures and overseeing the District's Change Management and Security Training processes.

Essential Functions: As defined under the Americans with Disabilities Act, may include any of the following tasks, knowledge, skills, and other characteristics. This list is ILLUSTRATIVE ONLY, and is not a comprehensive listing of all functions and tasks performed by incumbents of this class.

Duties and Responsibilities: Within the scope of college policies and procedures, this position:

Manages computer access account functions in compliance with documented standards and procedures for Identity and Access Management to include on-boarding, off-boarding, requests for permission changes, reviews/inspects computer accounts for compliance with standards, and performs corrective actions

Provides oversight of the District's IT Change Management process to ensure implementation is documented and in compliance with industry standards and regulations

Manages the District's Information Security Training program, ensuring timeliness and compliance with training requirements; produces periodic reports and analyzes them to ensure Security Training goals and compliance requirements are met

Maintains a detailed understanding of District IT processes and standards; analyzes District performance against the standards, reports findings, recommends corrective action, and where applicable, participates in process improvements

Operates assigned District IT computer account management and access management tools

Documents evidence to support external audit and regulatory compliance expectations of the District's Information Security Program; creates and updates process documentation as needed to support continuity of the IT Security Compliance Administrator function.

Performs other related duties as assigned

General Expectations: Employees are expected to accomplish assigned duties in an efficient, effective and competent manner and to strive for improvement and excellence in all work performed. Additionally, employees must understand the comprehensive role of the community college and cooperate and work harmoniously with students, faculty and staff, and the public. Employees will follow all college policies, rules, regulations and guidelines as they relate to this position.

Job Description



Education and Experience Requirements:

Associate's degree in Cyber Security, information technology or related field from an institution accredited by an institutional accrediting body of higher learning recognized by the US Department of Education
Two years related professional experience

An equivalent combination of education and/or experience from which comparable knowledge, skills and abilities have been achieved will be considered.

Knowledge, Skills and Abilities:

Knowledge of and ability to follow college policies and procedures
Knowledge of computer operating systems
Knowledge of enterprise local area networking technologies including Ethernet switches, IP routers, and modern firewalls
Knowledge of IT infrastructure services such as virtual infrastructure, directory services, Microsoft domain/file/print services, and web services
Knowledge of identity and access management principles such as least access, role based access control, multi-factor authentication, single sign on (SSO), and zero trust.
Knowledge of the fundamental IT concepts of change management, inventory management, configuration management, and patch and vulnerability management.
Skilled in the use of the MS Office suite of office productivity applications
Skill in presenting ideas and concepts orally and in writing
Skill in the use and configuration of operating systems and developing command line/shell scripts to automate complex tasks
Ability to learn and apply new technical skills as technology and security requirements evolve
Ability to communicate effectively, verbally and in writing, and to relate to others in a professional, helpful manner
Ability to relate to a diverse population and to maintain composure when faced with difficult situations
Ability to organize, prioritize, and follow multiple tasks through to completion with an attention to detail
Ability to work independently while contributing to team environment
Ability to effectively identify and resolve problems and to maintain strict confidentiality related to sensitive information
Ability to analyze problems, identify solutions, and take appropriate action to resolve problems
Ability to establish and maintain effective working relationships with other department staff, faculty, students and the public

Work Environment: Work is primarily performed under general supervision in a typical office setting with appropriate climate controls. Will require some work during evening and weekend hours and travel to district campuses.

Physical Requirements: Essential functions of this position require: manual dexterity, ability to communicate.

Sedentary Work: Exerting up to 10 pounds of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull or otherwise move objects, including the human body; involves sitting majority of time; walking and standing are required only occasionally and all other sedentary criteria are met

Mental Application: Utilizes memory for details, verbal instructions, emotional stability, critical thinking, adaptability and creative problem-solving skills are important

Reports to: Chief Information Security Officer

Disclaimer: The above statements describe the general nature, level, and type of work performed by the incumbent(s) assigned to this classification. They are not intended to be an exhaustive list of all responsibilities, demands, and skills required of personnel so classified. Job descriptions are not intended to and do not imply or create any employment, compensation, or contract rights to any person or persons. Management reserves the right to add, delete, or modify any and/or all provisions of this description at any time as needed without notice. This job description supersedes earlier versions.