JOB DESCRIPTION

Position Title: Chief Information Security Officer

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: EX16

Position Summary: The Chief Information Security Officer (CISO) is responsible for the development, implementation and maintenance of the college's information security program, facilitating information security compliance, advising senior leadership on security direction and resource investments, and establishing and implementing appropriate policies to manage information security risk.

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:

Responsible for the strategic and tactical leadership of the college's information security program

Manages college-wide information security governance processes, serves as chair of the Information Security Team, leads the establishment of an information security office, manages project priorities related to information security, and serves as primary lead for information security incident response

Establishes annual and long-range information security and compliance goals, defines information security strategies, metrics, reporting mechanisms and program services; and creates maturity models and a roadmap for continual program improvements

Leads the development and implementation of effective policies and practices to secure protected and sensitive data and ensures information security and compliance with relevant compliance laws, regulations and related requirements

Leads efforts to internally assess, evaluate, and make recommendations to senior administration regarding the adequacy of the security controls for the colleges information and technology systems

Responsible for supervising and directing the Director of Information Security Compliance; ensures that security and compliance activities and tasks are completed; and meet compliance requirements and deadlines; provides regular feedback and evaluation of performance and establishes goals and timelines for successful completion of projects and tasks

Oversees internal technology audits and works with government audit agencies, and outside consultants as appropriate on required information security assessments and audits

Coordinates and tracks all information security related audits including scope of audits, colleges/units involved, timelines, auditing agencies and outcomes, and provides guidance, evaluation and advocacy on audit responses

Works with college leadership to build a cohesive information security and compliance programs for the college to effectively address state and federal statutory and regulatory requirements

Stays informed of information security issues and regulatory changes affecting higher education at the state and national level, participates in national policy and practice discussions, and communicates to college leadership on a regular basis regarding topics.

Engages in professional development to maintain continual growth in professional skills and knowledge essential to the position

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.

Education and Experience Requirements:

Bachelor's degree in information security or a related field from an institution accredited by an institutional accrediting body of higher learning recognized by the US Department of Education

Five years of related experience in information security or a related field

Preference may be given to individuals with industry specific certifications, including GIAC/SANS (Global Information Assurance Certification/System Administration, Network, and Security), CISSP (Certified Information Systems Security Professional), CISM/A (Certified Information Security Manager/Auditor), CompTIA Security+, Certified Ethical Hacker, CCSP (Certified Cloud Security Professional)

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

Knowledge, Skills and Abilities:

Knowledge of and ability to follow college policies and procedures

Knowledge of Microsoft Office suite

Knowledge of state and federal information security regulatory requirements (GLBA, FERPA, etc.)

Knowledge of IT Security Frameworks (NIST, IHECF, etc.)

Skill communicating technical information to non-technical audiences both verbally and in writing

Skill in project management, time management, and initiation and execution of tasks

Skill in presenting ideas and concepts orally and in writing

Ability to communicate effectively, verbally and in writing, and to relate to others in a professional, helpful manner

Ability to assess cybersecurity policies, standards, and procedures for key cybersecurity concepts (access to programs and data, changes to programs and data, IT operations, etc.) in order to identify gaps with regulatory requirements (GLBA, FERPA, etc.) and information security frameworks (NIST, IHECF, etc.)

Ability to assess IT dependencies (system integrations, reports, segregation of duties, automated application controls, etc.) within information systems

Ability to communicate the impact of cybersecurity control effectiveness on business processes to nontechnical stakeholders

Ability to communicate gaps in cybersecurity control design to control owners and make meaningful recommendations

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 analyze problems, identify solutions, and take appropriate action to resolve problems using independent judgment and decision-making processes
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. Incumbent generally performs work in a typical office setting with appropriate climate controls. Work may require travel, early morning, evening, or weekend work.

Physical Requirements: Essential functions of this position require: lifting, 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 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.