JOB DESCRIPTION

Position Title: Director of Cybersecurity

Division: Business and Technology	**Employment Category:** Administrative Staff
Primary Location: District-wide Based at the Downtown Center	**FLSA Classification:** Exempt **Remote Eligible:** No
Parameters: Full-time; 12 Month	**Pay Grade:** AS18

Position Summary: The Director of Cybersecurity provides district wide administrative direction and leadership to the Cybersecurity program. Develops, implements, evaluates and maintains the Cybersecurity program in accordance with the appropriate accreditation and certification regulatory agencies and college standards. Cultivates relationships with local, state, regional and national Cybersecurity professionals, organizations and policy makers. This position requires the director to manage course schedules, Associate faculty, and strategic plans for the Cybersecurity program.

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:

Directs and supervises the work of all full-time faculty, part-time faculty, part-time staff and student workers within the Cybersecurity program. Develops and maintains both short-term and long-term budgets for the Cybersecurity program. Serves as the initial administrative contact for complaint resolution and/or grievances for faculty, staff and students. Provides guidance and direction on all Cybersecurity course schedules.

Provides ongoing program, course and lab evaluation for effectiveness. Ensures that the Cybersecurity program and courses meet both college and regulatory agency (NSA, HLC, etc.) requirements and standards. Applies and maintains standards of quality operating methods, processes, systems, and procedures; implements changes as necessary to maintain a successful Cybersecurity program; integrates knowledge of industry trends and professional training to continuously improve program quality

As needed may teach Cybersecurity course(s) and associated labs in accordance with the college's workload policy. Maintains written instructional standards; facilitates instruction using alternative delivery methods as needed; informs students in writing of instructional standards; posts and maintains office hours; participates in the assessment of student learning outcomes; establishes, maintains and submits accurate student and instructional records in a timely manner

Manages the fiscal and operational aspects of the Cybersecurity program, including labs. Manages the maintenance, troubleshooting, and building of hardware and software necessary for the successful deployment of all Cybersecurity courses. Participates in preparing grant and program proposals

Participates in department, division and college meetings; serves on college committees as assigned; participates as advisor for Cybersecurity student organizations, clubs, competitions and other student related activity

Serves as the liaison with state, industry, educational and governmental Cybersecurity professionals and programs; represents the college and the program at meetings, conferences and seminars; participates in professional organizations; represents the college and the program for all accrediting and certification related responsibilities

Participates in the recruitment of prospective Cybersecurity students; participates in strengthening relationships with external stakeholders such as industry partners; participates in the organization of department and program advisory council meetings

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:

Master's degree in Cybersecurity, or related discipline from a regionally accredited institution of higher learning recognized by the US Department of Education

Two years' related professional experience

Two years' successful teaching experience, preferably at a community college

Demonstrated leadership experience

Preferred Qualifications:

Five years related professional experience

Experience with NSA certification/recertification

Experience teaching using alternative delivery methods is desired.

Experience with use of technology in lecture and lab settings is preferred

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

Knowledge, Skills and Abilities:

Knowledge of and ability to follow college policies and procedures

Knowledge of trends, developments, new technologies affecting the Cybersecurity program

Knowledge of curriculum and program development

Knowledge of public relations/marketing practices and methods

Knowledge of computer networking concepts and protocols, and network security methodologies.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of virtualization technologies and virtual machine development and maintenance.

Skill in current technologies and word processing, database, presentation, and spreadsheet software, specifically Microsoft Office applications

Skill in instructing students from diverse cultures and/or backgrounds

Skill in applying security controls.

Skill in using authentic assessment to evaluate students' needs and progress

Skill in integrating technology into curriculum and other educational services

Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).

Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).

Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).

Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).

Skill in communicating with all levels of management including governing board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).

Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).

Ability to relate to a diverse population and to maintain composure when faced with difficult situations

Ability to multi-task and organize, prioritize, and follow multiple projects and tasks through to completion with an attention to detail

Ability to work independently while contributing to team environment

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

Ability to effectively identify and resolve problems and to maintain strict confidentiality related to sensitive information

Ability to analyze problems, identifies solutions, and takes 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

Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.

Ability to operate common network tools (e.g., ping, traceroute, nslookup).

Ability to understand technology, management, and leadership issues related to organization processes and problem solving.

Work Environment: Work is primarily performed under general supervision. Incumbent generally performs work in a typical classroom or laboratory setting with appropriate climate controls and includes exposure to mechanical and chemical hazards.

Physical Requirements: Essential functions of this position require: lifting, manual dexterity, ability to communicate and exposure to biological and chemical hazards.

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: Dean of Business and Technology

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.