Title:	Assistant Director, Information Security
Range:	17
Synopsis:	New Position
Rationale:	This position is essential to protect the College from emerging cyber threats. At a high level, they are responsible for evaluating, deploying, and managing risk-based assessments for systems, legal requirements, and industry best practices. They will also develop, implement, and maintain policies and procedures to ensure the confidentiality, integrity, and availability of College systems and oversee the information security training and awareness program, secure vendor evaluation and onboarding, and establish and maintain the College's Security Operations Center (SOC). This position oversees all information security operations and activities that are crucial for keeping the College's information systems and data secure and accessible.

ASSISTANT DIRECTOR, INFORMATION SECURITY

DEFINITION

Under administrative direction, plans, organizes, manages, and provides direction and oversight for all functions and activities related to information security for the College; directs the planning and implementation of enterprise information technology systems, business operations, and facility defenses against security breaches and vulnerability issues; responsible for auditing existing systems, while directing the administration of security policies, activities, and standards; develops security plans, user guidelines, and procedures; participates in infrastructure projects to ensure security and compliance requirements are met; assists to direct the implementation and upgrade of existing security practices and systems; promotes awareness of security policies to the campus; assesses and helps to reduce ongoing system security threats and vulnerabilities; monitors system and application compliance with security guidelines and standards; participates in directing the performance of incident response activities; provides highly responsible and complex professional assistance in areas of expertise.

SUPERVISION RECEIVED AND EXERCISED

Receives administrative direction from the assigned managerial personnel. Exercises direct and general supervision over assigned staff.

CLASS CHARACTERISTICS

This is a management classification in the Information Technology (IT) Department that assists in managing all activities of information security operations and activities. Responsibilities include performing diverse, specialized, and complex work involving significant accountability and decision-making responsibility. The incumbent organizes and oversees day-to-day activities and is responsible for providing professional-level support in a variety of areas. Assists in planning and development, and administration of departmental policies, procedures, and services. Successful performance of the work requires an extensive professional background, as well as, skill in coordinating departmental work with that of other departments.

EXAMPLES OF ESSENTIAL FUNCTIONS (Illustrative Only)

1. Leads strategic security planning to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment, and management of existing and future security technologies using a risk-based assessment methodology.
2. Collaborates with IT Infrastructure team to establish and maintain secure network architectural designs, firewalls, and network border security tools to address security for internal network and external internet connectivity.
3. Oversees systems design and development from business requirements analysis through to day-to-day management; plans and implements information security policies, standards, and operating procedures utilizing frameworks such as Center for Internet Security Critical Security Controls (CIS CSC), National Institute of Standards and Technology Special Publication (NIST SP), International Standard on requirements for information security management (ISO/IEC), and Control Objectives for Information and Related Technologies (COBIT).
4. Develops and communicates information security strategies and plans to the executive team, Board of Trustees, College leadership, faculty, staff, students, partners, and stakeholders. Acts as an advocate and liaison for the College's vision toward information security activities.
5. Assists with the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements. Performs continual business impact analysis for College systems and processes.
6. Develops, implements, maintains, and oversees enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.
7. Defines and communicates corporate plans, procedures, policies, and standards for the organization for acquiring, implementing, and operating new security systems, equipment, software, and other technologies.
8. Manages the administration of all computer security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
9. Manages the administration of the College security systems and their corresponding equipment or software, including industrial supervisory control and data acquisition systems (SCADA).
10. Develops, tracks, and controls the information security services' annual operating and capital budgets for purchasing, staffing, and operations.
11. Ensures that facilities, premises, and equipment adhere to all applicable laws and regulations.
12. Recommends and implements changes for information security policies and practices in accordance with changes in local or federal law; provides resolution to information security needs and requirements in a cost-effective manner.
13. Assesses and communicates any and all security risks associated with any and all purchases or practices performed by the College.

14. Collaborates with IT leadership, privacy officers, and Human Resources to establish and maintain a system for ensuring that security and privacy policies are met; promotes and oversees strategic information security relationships between internal resources and external entities, including government, vendors, and partner organizations.
15. Remains informed on trends and issues in the security industry, including current and emerging technologies and prices. Advises, counsels, and educates executive and management teams on their relative importance and fiscal impact.
16. Assists with the selection, training, motivation, and direction of department assigned personnel; evaluates and reviews work for acceptability and conformance with department standards, including program and project priorities and performance evaluations; works with employees on performance issues; implements discipline procedures; responds to staff questions and concerns.
17. Establishes, implements, and fosters an environment of belonging as it relates to diversity, equity, inclusion, social justice, anti-racism, and accessibility (DEISAA).
18. Oversees, leads, and provides quality customer service when interacting with the public, vendors, students, and College staff, including individuals from minoritized groups.
19. Utilizes critical thinking, sound decision-making, and problem-solving skills with tact, confidence, and diplomacy.
20. Implements, enforces, supports, and abides by federal, state, local policies, and Board Policies and Administrative Procedures.
21. Participates on and supports employee participation on committees, task forces, and special assignments, including, but not limited to Screening and Selection Committees and mandated trainings as required.
22. Prepares and delivers DEISAA-minded presentations related to assigned areas as required.
23. Performs other related duties as assigned consistent with the scope of the position.

QUALIFICATIONS

Knowledge of:

1. Principles and practices of supporting a diverse, equitable, inclusive, socially just, anti-racist, and accessible academic and work environment.
2. Principles and practices of employee supervision, including work planning, assignment, review and evaluation, and the training of staff in work procedures.
3. Principles and practices of public agency budget development and administration and sound fiscal management policies and procedures.
4. Proven experience in planning, organizing, and developing IT security and facility security system technologies.

5. Technology environments, including information security, building security, defense solutions, Role Based Access Controls, and zero trust architecture strategies.
6. Business theory, business processes, management, budgeting, and business office operations.
7. Data processing, hardware platforms, enterprise software applications, cloud and vendor hosted systems.
8. Computer systems characteristics, features, and integration capabilities.
9. Applicable federal, state, and local laws, regulatory codes, ordinances, and procedures relevant to assigned area of responsibility.
10. Principles and practices of employee supervision, including work planning, assignment, review and evaluation, and the training of staff in work procedures.
11. Modern office practices, methods, and computer equipment and applications related to the scope of responsibility.
12. Techniques for effectively representing the College in contacts with governmental agencies, community groups, and various business, professional, educational, regulatory, and legislative organizations.
13. Techniques for providing a high level of customer service by effectively interacting with the public, vendors, students, and College staff, including individuals of various ages, disabilities, socio-economic levels and ethnic groups.

Skills & Abilities to:

1. Implement, advocate for, and communicate the College's vision and commitment to creating a diverse, equitable, inclusive, socially just, anti-racist, and accessible academic and work environment.
2. Oversee and address gaps in diversity, equity, inclusion, social justice, anti-racism, and accessibility in recruitment and retention of faculty, management, and staff.
3. Exercise critical thinking and sound decision-making through observing, analyzing, inferring, communicating, and problem-solving in challenging situations with ethics, tact, confidence, and diplomacy.
4. Develop and implement resources and strategies towards the goal of being diverse, equitable, inclusive, socially just, anti-racist, and accessible in academic and work environments.
5. Participate in the design, management, and security of a comprehensive, College-wide, state-of-the-art network infrastructure/services.
6. Perform technical specification, design, implementation, and integration on network services in support of Instructional, Student Services, Administrative, and Community Support initiatives and goals.
7. Interpret, apply, explain, and ensure compliance with federal, state, and local policies, procedures, laws, and regulations.
8. Plan, organize, direct, and coordinate the work of supervisory, professional, and technical personnel; delegate authority and responsibility.

9. Prepare clear and concise reports, correspondence, policies, procedures, and other written materials.
10. Organize and prioritize a variety of projects and multiple tasks in an effective and timely manner; organize own work, set priorities, and meet critical time deadlines.
11. Communicate effectively through various modalities.
12. Establish and maintain a variety of filing, record-keeping, and tracking systems.
13. Understand scope of authority in making independent decisions; review situations accurately and determine appropriate course of action using judgment according to established policies and procedures.
14. Learn and apply emerging technologies and, as necessary, to perform duties in an efficient, organized, and timely manner.
15. Review situations accurately and determine appropriate course of action using judgment according to established policies and procedures; understands scope of authority in making independent decisions.
16. Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:

1. Equivalent to a bachelor's degree from a regionally or nationally accredited four-year college or university with major coursework in computer science, management information systems, Computer Information System (CIS), Information Technology (IT), business administration, organizational behavior, or a related field, and
2. Three (3) years of increasingly responsible leadership and technology support experience in information technology.

Desirable Qualifications:

1. Current Certified Information Systems Security Professional (CISSP) certificate or equivalent industry certification (ex. Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA).
2. Proven track record of implementing or overseeing programs or policies relating to diversity, equity, inclusion, anti-racism, and accessibility preferably in a minority serving institution such as Hispanic Serving Institution (HSI) and Asian American and Native American Pacific Islander-Serving Institution (AANAPISI); OR
3. Proven track record of participating in programs relating to diversity, equity, inclusion, anti-racism, and accessibility preferably in a minority serving institution such as Hispanic Serving Institution (HSI) and Asian American and Native American Pacific Islander-Serving Institution (AANAPISI).

Licenses and Certifications:

The incumbent may periodically be required to travel to a variety of locations. If operating a vehicle, incumbents must have the ability to secure and maintain a valid California driver's license.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and to visit various College sites; vision to read printed materials and a computer screen; and hearing and speech to communicate in person, before groups, and over the telephone. This is primarily a sedentary office classification although standing and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Incumbents must possess the ability to lift, carry, push, and pull materials and objects up to 20 pounds.

ENVIRONMENTAL ELEMENTS

Incumbents work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Incumbents may interact with upset staff and/or public and private representatives in interpreting and enforcing departmental policies and procedures.