Cerritos College Job Description

Position: Manager, Information Technology Security

Grade: 28 (Management Salary Schedule)

Summary

Plans, supervises, assesses evaluates, and participates in activities dedicated to providing technical support, maintenance, security, and troubleshooting to district users on hardware and software applications used for administrative and academic purposes, including ERP systems. Oversees and provides advanced technical guidance to staff on a wide variety of complicated installations, upgrades, repairs, and implementations. Supervises, maintains, and oversees all centralized equipment within the computer room.

The Manager of Information Technology Security will be held accountable for the following:

- Assessing risks, threats, technologies, architecture
- Recommending improvement strategies for identified gaps
- Developing, coordinating, and leading Incident Response
- Developing an Information Technology Security Plan and Policies
- Monitoring and compliance
- Implementing an End-user education and awareness program

Distinguishing Career Features

The Manager, Information Technology Security reports to the Director, Information Technology and is responsible for risk assessment, policy, technical standards, configuration, and system security. This position also provides complex administrative support to the Director, Information Technology.

Essential Duties and Responsibilities

- Work with academic and business units to facilitate Information Technology risk assessment and risk management processes; this includes identifying location, type, sensitivity, ownership, and access requirements for data being used.

- Participates with the Network Administrator and Director, Information Technology in planning and design of security infrastructure. Participates in business and strategic planning for the department and in the assessment of organizational effectiveness.

- Monitor the external threat environment for emerging threats and advise on appropriate course of action.

- Research, identify, coordinate, and play key role in the implementation of appropriate Information Technology security systems, technology and controls including firewalls, intrusion detection/prevention and vulnerability scanners.

- Research and disseminate amongst Information Technology personnel Information

Technology security best practices and resource information.

- Provides leadership in the new and emerging technologies in support of campus information technology security.

- Develop, implement, and manage Information Technology security incident response processes and procedures.

- Develop, implement, and maintain an Information Technology security plan to ensure the integrity and confidentiality of information residing on Cerritos workstations, servers, mobile devices, and related computer peripherals.

- Develop, implement, maintain, disseminate, and oversee enforcement of Information Technology security related policies and procedures.

- Leads, supervises, trains, and evaluates assigned personnel. Certifies payroll for assigned personnel. Applies the terms and provisions of applicable collective bargaining agreements; state and federal laws; and District Board Policies and Administrative Procedures in personnel matters.

- Maintain an in-depth technical documentation repository of Cerritos College systems, networks, and core applications.

- Coordinate, report on, document and act on results of periodic (annual) Information Technology security audits.

- Develop and implement strategies for complying with applicable Federal, State, and other legal compliance requirements related to Information Technology Security.

- Develop, implement, and manage an Information Technology security awareness and training program.

- Assist with the development and implementation of business continuity and disaster recovery plans.

- Participate as a member of Information Technology management team in the development, prioritizing, budgeting, and planning of Information Technology security strategies and related initiatives.

- Develop and communicate current Information Technology security posture status, Information Technology security strategies, and progress on Information Technology security initiatives to key organizational units, executive management, and Board of Trustees.

- Manages information security. Research new techniques and enhancements for data, servers, and networks to be secure.

- Performs formal presentations to inform, educate, and maintain communication with staff, faculty, and or administration. Provides web-based documentation as appropriate.

- Collaborate with other colleges and universities to share information or resources, as necessary, and to improve overall security of the higher education sector.

- Keep current with Information Technology security industry research and best practices related to keeping an organization's Information Technology systems and networks appropriately secure. This includes attending conferences and training as required to maintain Information Technology security management proficiency.

- Develop and manage relationships with Information Technology security vendors and consultants and recommend as appropriate solutions and partnerships that would benefit Cerritos in its Information Technology security efforts.

- Perform other duties as assigned.

Qualifications

Minimum Qualifications for Education and Experience:

1. Bachelor's degree with a concentration in one or more of the following areas: Computer Science, Information Technology, Networking, Microcomputer Hardware and Software Components, Microcomputer Operating Systems, Data Communications Software, or a related area,

2. Five or more years of experience in Information Technology Networks, Systems or Security related position, and

3. Understanding of and sensitivity to meeting the needs of the diverse academic, socioeconomic, cultural, disability and ethnic background of the student, community, and employee population (E.C. 87360a).

Preferred Qualifications:

1. Certifications such as CISSP (Certified Information System Security Professional), CISM (ISACA Certified Information Security Manager) or CISA (ISACA Certified Information Security Auditor) are preferred.

2. Master's Degree in cybersecurity or related fields.

Knowledge and Abilities

Knowledge and Skills

The position requires professional knowledge of:

- Ability to identify, analyze, prioritize, and communicate impact of Information Technology security risks and exposures.
- Understanding of effective Information Technology security system and network architectures, concepts, techniques, and tools.
- Understanding and experience managing network and system security components

such as firewalls and intrusion detection/prevention systems.

- Experience in organizing, prioritizing, developing, implementing and communicating status on Information Technology security strategies and projects.
- Proficiency in Information Technology security management, industry best practices and standards.
- Experience developing and implementing Information Technology security policies and procedures.
- Experience in and knowledge of Information Technology security auditing and monitoring.
- Knowledge of and experience meeting applicable Information Technology security related laws and regulations.
- Ability to develop, learn and implement new concepts, technologies, and methods.
- Knowledge of and exposure in developing and testing business continuity and disaster recovery plans.
- Exposure to the operation of institution wide networks, systems and applications.
- Ability to follow-up and follow-through in a coordinating role across multiple constituencies to achieve tactical and strategic goals.
- Excellent analytical, planning, and organizational skills.
- Agility in adapting to and thriving in a dynamic work environment including shifting of project objectives, deadlines, resources and priorities.
- Ability to work effectively with administrators, faculty and staff.
- Excellent oral and written communication skills.
- Knowledge and experience in data privacy like CCPA, FERPA, PCI, and HIPPA.
- Familiarity with emerging technologies such as AI and machine learning in cybersecurity, as well as cloud security practices.
- Experience with incident response planning and related activities.

The position requires demonstrated skill in:

- Organizing work and building an effective team to meet the needs of the assigned areas.
- Oral and written language sufficient to prepare reports and professional correspondence.
- Human relations/interpersonal skills to conduct performance reviews, deliver presentations, and convey technical information to a wide variety of audiences.
- Familiarity with cybersecurity frameworks like NIST, ISO 27001, the MITRE Framework, or CIS Controls, to ensure knowledge of and alignment with industry standards.

Abilities

This position requires the ability to:

- Be open to change and new methods in the assigned area of responsibility.
- Continuously engage in learning and self-improvement.
- Meet change with innovation to promote and meet the college mission.
- Organize, plan, develop, and write new programs, develop new concepts, analyze outcomes, and prepare clear and concise reports.
- Guide and direct others in goal achievement.
- Direct and facilitate development of personal and team perspectives and develop and deliver training programs.

- Develop and monitor budgets and maximize financial resources.
- Work cooperatively and productively with internal and external constituencies.
- Advocate for shared governance, collegiality, staff cohesiveness and for the core values of the institution.
- Develop formal plans pertaining to personal, administrative, and academic computing, and organize, prioritize, and delegate work assignments.
- Translate user requirements into computer applications and systems.
- Coordinate applications development functions and steps and follow logical progressions for programming systems.
- Analyze and evaluate the needs of users and develop the most effective program or solution to meet those needs.
- Direct and design logical and physical database structures and relationships, including those for networked and web-based systems.

Physical Abilities
This position requires the physical ability to:

- Function in an office environment performing work of primarily a sedentary nature with some requirement to move about campus and to off-campus locales.
- The person in this position frequently communicates with members of the campus community. Must be able to exchange accurate information in these situations.
- Must be able to recognize printed material (printed or online) for more than 50% of the expected work time.
- Constantly operates a computer and other office productivity machinery, such as a calculator, copy machine, and computer printer.
- Requires the ability to lift, push, and pull objects of medium weight (less than 30 lbs.) on an occasional basis with or without accommodation.
- Work a flexible schedule which may include evenings, weekends, and split schedules.

Licenses and Certificates
May require a valid driver's license.

Working Conditions

Work is performed indoors where minimal safety considerations exist.

Presented for Board Approval: January 24, 2024