YOSEMITE COMMUNITY COLLEGE DISTRICT *Range 42*

DIRECTOR OF INFORMATION SECURITY

DEFINITION

Under the direction of the Vice Chancellor of Information Technology and Institutional Research, the Director of Information Security designs, implements, and supports the security and infrastructure of District systems, servers, peripherals and network devices. This role also analyzes, plans, designs, implements, maintains, troubleshoots and enhances networks security systems, processes and policies. This includes but is not limited to server virtualization, LANs, WANs, wireless technologies and the physical and logical components that integrate these systems together.

SUPERVISION RECEIVED AND EXERCISED

The Director of Information Security reports directly to a District executive and may provide support to IT managers and to numerous professional, technical as well as other administrative support staff.

ESSENTIAL DUTIES

- Serve as the Chief Information Security Officer (CISO) for the District
- Ensure appropriate security policies, NIST and CIS controls, are applied to all workstations, devices, infrastructure and server systems
- Perform routine security audits and oversee mitigating any risks that come out of the audits
- Serve as the main point of contact and lead law enforcement and other authorities in the event of a cybersecurity incident
- Compose and report on the District's cybersecurity stance to the Chancellor, Board of Trustees, colleges, accreditation and audit reports as needed
- Lead in the creation and updating of security related board policies and administrative procedures ensuring security policies are applied correctly and meet current requirements
- Serve as the main point of contact for outsourced managed security operations center or managed detection and response
- Manage and maintain the District's security event information system (SEIM) and data loss prevention software
- Work with all areas of the IT department to ensure appropriate security policies are implemented
- Lead in updating District's incident response plan, responds to any cyber incidents or events that occur in accordance with the District's incident response plan
- Assist in developing and maintaining relevant sections of the District's continuity plan
- Design, plan, test, implement and document complex security enhancements and additions to the network infrastructure
- Provide high level support of the District's technology infrastructure including but

not limited to firewalls, backup, and disaster recovery systems
- Perform or direct security upgrades on the District's critical IT infrastructure
- Recommend and implement security polices, protocols, practices and lead in the creation of security training and guidance to staff
- Provide guidance and mentoring to Network Specialists and other IT staff
- Develop and maintain the technical expertise needed to meet long-term business needs
- Coordinate security related projects and work activities between operations, applications and systems staff
- Implement system software/hardware standards, upgrade procedures and maintenance activities to meet reliability, security, accessibility standards and expectations
- Develop security related technology replacement life-cycle and budget
- Troubleshoot network hardware and operating problems, including but not limited to connectivity, internet access, email and servers
- Develop and maintain complete and accurate records pertaining to hardware, software, system, and network configurations, changes, outages and improvement plans
- Compile data and perform analysis as directed
- Maintain current knowledge with advances in security standards and best practices and recommend new technologies and/or upgrades to current technologies to improve security
- Work collaboratively and cooperatively with all levels of administration, faculty, staff and student workers
- Provide training and support on IT and network security related matters
- Directs data compilation and performs analysis as needed or directed
- Directs the work outcomes of other technical support staff and provides performance feedback to supervisors
- Performs related duties as assigned

MINIMUM QUALIFICATIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The Education/Experience, Knowledge and Ability requirements are representative of essential duties. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions of the position.

Education and Experience:

- **Education:** A Bachelor's Degree from an accredited College or University in Information Technology, Information Security, Cybersecurity or a related field. A Master's Degree in a related field is preferred
- **Experience:** Five (5) years of increasingly responsible experience securing network and server/storage infrastructures in support of multi-campus network with a demonstrated work history of increasingly responsible positions in Information Technology, experience in an academic environment in a leadership role and history of having a strong, open, collaborative

leadership style.

Knowledge of:
- Methods and procedures of standardizing, securing, maintaining, and operating computers and peripheral equipment in an enterprise environment
- Software License compliance laws and methodologies
- Microsoft Active Directory and Azure Active Directory
- Current server virtualization, network switching and routing, firewalls, data backup and recovery solutions, cloud computing resources, VoIP systems, business software applications (e.g. Office 365), and related systems used by the District
- Security and business continuity (disaster recovery and backup) planning and execution
- Troubleshooting, diagnostic techniques, procedures, equipment and tools used in computer and peripheral repair
- Technology documentation and presentation techniques
- Project management methods and techniques
- Supervisory knowledge and/or experience to successfully oversee a team, while providing complex project coordination across departments
- Professional and effective oral and written communication at all times
- Current NIST standards and CIS controls

Ability to:
- Apply current NIST and CISO standards to current operations
- Delegate, plan, schedule and perform complex maintenance and upgrades to critical infrastructure
- Respond to incidents and events, implement appropriate counter measures to maintain and protect security of district data.
- Plan, schedule and perform complex maintenance and upgrades to critical infrastructure
- Maintain current knowledge of technical advances in all areas of responsibility
- Prepare clear, concise, and accurate system documentation and reports
- Establish and maintain cooperative and effective working relationships with IT staff, members of the District community and outside contacts
- Analyze networking systems to modify current standards and develop innovative solutions to address changing conditions
- Demonstrate interpersonal skills using tact, patience, and courtesy
- Understand and carry out oral and written directions
- Direct the work of other technical support employees
- Supervise staff as assigned
- Create and maintain positive business relationships with the broader District community and third-party vendors
- Manage and track budgets
- Demonstrate sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students and employees

Licenses and Certificates:

- SSCP – Systems Security Certified Practitioner
- CISSP – Certified Information Systems Security Professional
- Possession of a valid California Motor Vehicle Operator's License

Physical and Mental Standards:

- **Mobility:** ability to sit for long periods, move about an office, stand occasionally, reach above and below desk level.
- **Dexterity:** fine manipulation sufficient to operate a computer keyboard, handle individual papers, write and take notes.
- **Visual Requirements:** close vision sufficient to read files, documents, and computer screens and do close-up work; ability to adjust focus frequently.
- **Hearing/Talking:** ability to hear normal speech; speak and hear on the telephone, and speak in person.
- **Emotional/Psychological Factors:** ability to make decisions and concentrate; frequent contact with others including some public contact; frequent deadlines and time-limited assignments.

TYPICAL WORKING CONDTIONS

- Work is generally performed in a standard office environment with some travel to different sites.
- Work may require evening and weekend hours.

Class Adopted: January 2024
Class Amended: