DESERT COMMUNITY COLLEGE DISTRICT

DIRECTOR, INFORMATION SECURITY

POSITION DESCRIPTION

The Director of Information Security is responsible for the development, implementation, and management of a comprehensive, District-wide information security and data privacy program. This is a senior leadership position responsible for protecting the confidentiality, integrity, and availability of all institutional information assets.

The Director provides strategic guidance and operational oversight for all aspects of cybersecurity, including risk management, security architecture, incident response, vulnerability management, and regulatory compliance. This role is responsible for establishing security policies and standards, promoting a culture of security awareness, and leading the District's response to all information security incidents. The Director works collaboratively with all district departments to ensure that security is integrated into all technology-related activities, safeguarding the District's mission-critical operations and the data of its students, faculty, and staff.

SUPERVISION RECEIVED AND EXERCISED

Receives direct supervision from Chief Technology Officer or designee. Exercises supervision over assigned personnel. The incumbent is expected to work independently, exercising professional judgment and initiative to achieve departmental goals. Exercises direct supervision over assigned technical, clerical, and support personnel.

REPRESENTATIVE DUTIES/ESSENTIAL FUNCTIONS

The duties listed are intended to provide examples of the types of work performed and are not intended to be an exhaustive list of all responsibilities. The District reserves the right to modify or assign additional duties consistent with the classification.

The following duties are representative of the essential functions of this position:

1. Define the strategic direction for information security governance; review and authorize all information security policies and standards to ensure alignment with institutional goals and risk appetite; serve as the primary expert on security matters for college leadership.
2. Oversee the District's Enterprise Risk Management (ERM) function for IT; analyze aggregate risk data to report critical exposures and strategic recommendations to the Chief Technology Officer.
3. Ensure institutional compliance with federal and state laws and regulations pertaining to information security and data privacy, including, but not limited to, Family Educational Rights and Privacy Act (FERPA), California Consumer Privacy Act (CCPA), Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry/ Data Security Standards (PCI DSS).
4. Develop and manage the District-wide security awareness and training program for all students, faculty, and staff.

5. Lead the District's security incident response team. Develop and maintain the official Incident Response Plan (IRP), and act as the incident commander during security events, from initial detection through to remediation and reporting.
6. Oversee and monitor the District networks and systems for security threats and anomalies. Manage security tools such as Security Information and Event Management (SIEM), firewalls, and intrusion detection/prevention systems.
7. Direct the District's vulnerability management program, including regular scanning, risk prioritization, and coordination of patching and remediation efforts with other IT teams.
8. Conduct and/or oversee digital forensics investigations in response to security incidents or policy violations.
9. Serve as the lead security architect, providing guidance to the infrastructure and application teams to ensure security is built into the design and implementation of all new systems and services.
10. Collaborate with the Enterprise Applications team on the security of the Student Information System (SIS) and other critical applications.
11. Coordinate with departments to ensure that data is classified and handled appropriately based on its sensitivity.
    Serve as the executive lead for security audits; negotiate audit scope, authorize management responses to findings, and accept final accountability for the remediation of identified risks.
12. Assist with the planning and monitoring of the departmental budget, including the procurement of endpoint hardware, software licenses, and audio-visual equipment.
13. Chair or Co-Chair assigned governance committees to create policies and standards for data quality, access, and usage.
14. Provide direct supervision, coaching, and professional development to assigned staff and student workers; conduct formal performance evaluations and recommend disciplinary actions in accordance with District policies and collective bargaining agreements.
    Develop and implement training programs to ensure a culture of professional, empathetic, and effective customer service across all user interactions.
15. Perform other duties as assigned.

KNOWLEDGE AND ABILITIES

Knowledge of:

- Comprehensive knowledge of information security principles, practices, and technologies.
- Leading security frameworks and standards National Institution of Standards and Technology (NIST) Cyber Security Framework (CSF), International Organization for Standardization (ISO 27001), Computer Information System (CIS) Controls.
- State and federal regulations governing data privacy and security in higher education (FERPA, GLBA, PCI DSS, CCPA).
- Incident response procedures, digital forensics, and threat intelligence.
- Security architecture for on-premise, cloud (SaaS, IaaS), and hybrid environments.
- Vulnerability management, patch management, and secure software development lifecycle.

- Network security technologies (firewalls, IDS/IPS, VPNs) and Identity and Access Management (IAM) solutions, including Multi-Factor Authentication (MFA).
- Cultural competency and an understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty, and staff.

Ability to:

- Demonstrate sensitivity to and an understanding of the diverse academic, socioeconomic, cultural, disability, and ethnic backgrounds of community college students and staff.
- Develop and implement comprehensive, enterprise-wide security policies and procedures.
- Maintain regular, reliable, and punctual attendance consistent with District standards and operational needs.
- Create and maintain standardized technical documentation, Standard Operating Procedures (SOPs), and knowledge base resources for the campus community.
- Supervise, coach, evaluate and motivate a team of technical professionals and foster a collaborative, customer-focused team culture.
- Establish and maintain cooperative and effective working relationships with others; work independently and confidentially with minimal direction; and exercise tact and diplomacy when handling sensitive or confidential matters.
- Interpret, apply, and explain rules, regulations, policies, and procedures; maintain records and prepare reports.
- Lead a formal incident response effort.
- Conduct thorough and objective risk assessments.
- Communicate effectively and professionally, both verbally and in writing, with users, technicians and District leadership and stakeholders, especially during stressful situations; de-escalate difficult customer interactions with empathy and tact. Analyze and manage multiple complex technical projects and develop effective solutions simultaneously.
- Foster a collaborative and security-conscious culture.

MINIMUM QUALIFICATIONS

Any combination of education and experience:

A Bachelor's degree from an accredited institution in Information Security, Computer Science, or a related field.

Seven (7) years of progressively responsible experience in information technology, with at least four (4) years focused specifically in a dedicated cybersecurity role.

Two (2) years of experience in a supervisory or leadership capacity.

OR

An Associate's degree from an accredited institution in Information Security, Computer Science, or a related field.

Nine (9) years of progressively responsible experience in information technology, with at least four (4) years focused specifically in a dedicated cybersecurity role.

Two (2) years of experience in a supervisory or leadership capacity.

WORKING CONDITIONS

Environment: District office environment; subject to constant interruptions and frequent interaction with others; sitting for long periods at a time (up to 2-3 hours); repetitive use of upper extremities including hand coordination activities; requires some evening and weekend responsibility; occasional travel to other locations to attend meetings or conduct work. The ability to type, use phone, stand intermittently, walk, bend and stoop, occasionally lift (up to 20 pounds), carry, push, pull or otherwise move objects of light to moderate weight, work at a computer, including sitting and viewing a monitor for various lengths of time, repetitive use of keyboard, mouse or other control device, dexterity of hands and fingers to operate keyboard, ability to communicate and provide information to others.

EMPLOYMENT STATUS

Classified Supervisor
Leadership Salary Schedule: Range 10
Personnel Management Committee Review: June 4, 2026
Board Approved: June 25, 2026