Desert Community College District
Information Security Officer

Basic Function

Provides technical expertise, coordination and planning in support of Information Technology (IT) security systems and initiatives. This position is responsible for security architecture, end point security, application security, database security, identity management, and infrastructure security.

Supervision Received and Exercised

Receives general supervision from assigned information technology senior leadership.

Examples of Typical Job Functions

1. Serves as the security engineer supporting security initiatives district-wide by designing and deploying information security technologies; advises IT staff on IT security matters; designs, develops, tests, installs, monitors, and maintains IT security systems for the district; enforces directives as mandated by regulations and state and federal law.
2. Plans, coordinates, and conducts major projects or phases of security projects;
3. Plans and coordinates monitoring, diagnosing, troubleshooting and resolving IT Security related support requests, including security problems/breaches.
4. Conducts and initiates security scans, audits, and performs risk assessments.
5. Researches, selects, plans, implements and supports effective IT Security controls, monitoring tools and practices; researches and recommends and facilitate IT Security Standards systems and

networks.

6. Performs technical security design/review activities for applications, networks, servers, architecture, and databases to ensure secure deployments.
7. Provides incident response and remediation support and initiates and coordinates with necessary vendors as required.
8. Monitors the external IT Security threat environment for emerging threats and make recommendations on appropriate course of action.
9. Conducts testing of simulated cyber-attacks to locate within IT systems vulnerabilities and mitigate.
10. Communicates trending risks and assists with developing, maintaining, and presenting IT Security awareness training for staff and faculty.
11. Assists with developing and maintaining documentation for IT Security architecture and programs policies and procedures; assists in designing and deploying multiple information security technology standards and procedures; ensures the adoption of information security requirements into the design, implementation, and operations within the system development life cycle.
12. Creates, updates, and coordinates all disaster recovery and related activities including testing and validation for restoration.
13. Promotes acceptance of security technologies within the organization, balancing business goals, security controls, and customer usability. Work with business management to communicate security risk and countermeasures.
14. Acts as the lead for technical personnel, third party vendors, auditors, investigators, and law enforcement agencies as required; assists and supports with all aspects of planning, design, development, coding, testing, debugging and implementation of complex systems

administration for a variety of operating systems.

15. Performs other related duties as assigned.

Qualifications

Knowledge of

1. IT architecture including data centers, cloud deployment, and containers.
2. Computer forensics and incident response tools and procedures.
3. Security standards and frameworks.
4. Knowledge of information technology security standards and requirements, trends and tools, LAN/WAN networks, operating systems, and ERP systems.
5. Design, develop and implement security solutions for complex and large networks.
6. Integrating security protocols to complex solutions and understanding relationships between applications.
7. Demonstrate working knowledge of the principles, practices and techniques of database structures and computer programming.
8. Working knowledge of firewalls, intrusion detection and prevention systems, auditing and scanning systems, VPN, and remote access systems.
9. Ability to provide guidance for the design and replacement of security related technologies.
10. Familiarity with information security regulations such as FERPA, HIPPA, PCI compliance.
11. Strong written and verbal communication skills, leadership, teamwork, and agility are critical success factors.

Ability to

1. Establish and maintain cooperative and effective working relationships with others.
2. Ability to provide security expertise and technical guidance to the District.
3. Apply independent technical judgment to complex technical situations.
4. Maintain current knowledge of technological advances in the security and related fields and current and emerging threats and technologies.
5. Communicate effectively both orally and in writing.
6. Maintain records and prepare reports.
7. Prioritize and schedule work. Analyze situations accurately and adopt an effective course of action.
8. Work independently with little direction and provide work directions to others.
9. Provide lead direction to short-term staff and/or student workers.
10. Demonstrate understanding of, sensitivity to, and respect for the diverse academic, socioeconomic, ethnic, religious, and cultural backgrounds, disability, and sexual orientation of community college students, faculty, and staff.

Education and Experience

A bachelor's degree in Information Technology, Computer Science, Business Administration, or a related field and five (5) years of progressively responsible experience in security, network design and development, computer forensics, technology related auditing, computer systems, and/or programming responsibilities.

Preferred Certifications

One or more relevant technical security certifications such as Certified Information Systems Security Professional (CISSP), Cisco CyberOps Professional, Certified Ethical Hacker (CEH), COMPTIA CySa+, or Offensive Security Certified Professional (OSCP).

Environment

Office environment.

Employment Status

- Bargaining Unit Position

Range 22

BOT Approved:8/16/2022