RANCHO SANTIAGO COMMUNITY COLLEGE DISTRICT CLASS SPECIFICATION
SANTA ANA, CALIFORNIA JULY 2017

INFORMATION SECURITY SPECIALIST

CLASS SUMMARY

Under minimum direction, will be responsible for security architecture, end point security, application security, database security, identity management, and infrastructure security. This position requires a thorough understanding of current and emerging threats and technologies for either on premise or in the cloud. In addition, the successful candidate will be responsible for designing and deploying information security technologies to directly support the efforts in securing the District's information or electronic assets and enforcing directives as mandated by regulations and state and federal law. Responsible for resolving the most complex security problems or breaches; conducts and initiates security scans, audits, and performs risk assessments. Acts as a liaison for interacting with third party vendors, forensic specialists, auditors, law enforcement, and/or investigations. Continuous involvement with all Information Technology Services Director's and the District's management team is required. Strong written and verbal communication skills, leadership, teamwork, and agility are critical success factors.

REPRESENTATIVE DUTIES

Design, deploy, and manage multiple information security technology standards and procedures. The technologies include end point security, application security, database security, infrastructure security, and identity management solutions; Provides incident response and remediation support and initiates and oversees necessary vendors as required; Perform technical security design/review activities for applications, networks, servers, architecture, and databases to ensure secure deployments for either on premise or cloud; Ensure the adoption of information security requirements into the design, implementation, and operations within the system development life cycle; Creates, updates, and oversees all disaster recovery and related activities including testing and validation for restoration for both on premise and in the cloud; Promote 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; Communicates trending risks with District employees and performs or provides training to mitigate the risk for the human factor; Acts as the technical lead for security vendors, investigators, and law enforcement agencies as required; Assists and supports all technical personnel with all aspects of planning, design, development, coding, testing, debugging and implementation of complex systems administration for a variety of operating systems; Assist with the development of bid specifications for acquisitions of network, data security, and telecommunications related equipment and services; Assist in the development of policies and procedures to ensure ongoing continuity. Develop and document security standards; Performs other related duties as assigned.

ORGANIZATIONAL RELATIONSHIPS

Information Security Specialist reports to designated manager of the Information Technology Services department.

INFORMATION SECURITY SPECIALIST continued

DESIRABLE QUALIFICATION GUIDE

Training and Experience

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

Knowledge

Knowledge of information technology security standards and requirements, trends and tools, LAN/WAN networks, operating systems, and ERP systems; Design, develop and implement security solutions for complex and large networks; Integrating security protocols to complex solutions and understanding relationships between applications; Demonstrate working knowledge of the principles, practices and techniques of database structures and computer programming; Working knowledge of firewalls, intrusion detection and prevention systems, auditing and scanning systems, VPN, and remote access systems. Ability to provide guidance for the design and replacement of security related technologies; Familiarity with information security regulations such as FERPA, HIPPA, PCI compliance.

Abilities

Ability to provide leadership and technical guidance to the District; plan, lead, coordinate and conduct major projects or phases of projects; Apply independent technical judgment to complex technical situations; Coordinate schedules and resources with systems and network programmers, engineers, users, technical services staff, risk management, campus management, and/or district safety; Diagnose and quickly respond to and resolve security breaches and understand reasons for systems failures; Maintain current knowledge of technological advances in the security and related fields; Communicate effectively both orally and in writing. Maintain records and prepare reports; Prioritize and schedule work. Analyze situations accurately and adopt an effective course of action; Work independently with little direction and provide work directions to others; Demonstrate understanding of, sensitivity to, and respect for the diverse academic, socio-economic, ethnic, religious, and cultural backgrounds, disability, and sexual orientation of community college students, faculty and staff.

WORKING CONDITIONS

This position requires ability to use computer workstations throughout the workday.