SANTA ROSA JUNIOR COLLEGE

TITLE: Manager, Network Security

CLASSIFICATION: Management Team – Classified Supervisor

SALARY RANGE: 24

SCOPE OF POSITION:

Under the direction of the Senior Director, Information Technology, leads a team to provide proactive security of District technology assets. The incumbent develops technology security guidelines, best-practice procedures, and supporting documentation to ensure the safety of the all electronic assets of the college; interacts with a diverse group of individuals including District management, business partners, external law enforcement and other regulatory agencies; and organizes and directs, trains, supervises and evaluates the performance of assigned staff.

KEY DUTIES AND RESPONSIBILITIES:

Examples of key duties are interpreted as being descriptive and not restrictive in nature. Incumbents routinely perform approximately 80% of the duties below.

1. Leads creation and management of District Information Security Policies including data security and backup and recovery plans; makes recommendations on training, policies, practices and software to improve security and operational efficiency at reasonable costs relative to the risks and staffing.
2. Manages security application systems and tools including virus protection, malware, zero day exploit protection and mitigation; technical asset management, user authentication, and intrusion prevention and detection; serves as a contributor in defining system security and functionality for other business system applications.
3. Conducts vulnerability threat assessments on existing and planned application systems and develops action plans to mitigate security gaps.
4. Trains, supervises and evaluates the performance of assigned staff; interviews and selects employees and recommends transfers, reassignments, terminations and disciplinary actions.
5. Stays current with technological changes that affect the security of the network, computers, and other equipment and evaluates and recommends vendor products to enhance District security.
6. Communicates with faculty, staff, students and external organizations to coordinate activities and programs; resolves issues and exchanges information.
7. Develops and prepares assigned information technology budgets and reports; analyzes and reviews budgetary and financial data; authorizes expenditures in accordance with established limitations.

KNOWLEDGE OF:

1. Information technology security standards and requirements, trends and tools, LAN/WAN networks, operating systems, and ERP systems
2. Security solutions for complex and large networks; Integrating security protocols to complex solutions and understanding relationships between applications;
3. Principles, practices and techniques of database structures and computer programming, computer server architecture (LINUX and Windows), network architecture, and virtualization.

KNOWLEDGE OF – Continued

4. Firewalls, intrusion detection and prevention systems, auditing and scanning systems, Virtual Private Networks (VPN), Public Key Infrastructure (PKI) and remote access systems.
5. Waterfall/Agile/Scrum development, and other applicable practices for technology management.
6. Budget preparation and control.
7. Principles and practices of administration, supervision and training.
8. Applicable laws, codes, regulations, policies and procedures, including FERPA, HIPPA, and PCI.
9. Interpersonal skills using tact, patience and courtesy.

Preferred Knowledge:

Commercial firewalls, patch management, Cisco network infrastructure, Amazon Web Services and other cloud service backup, cyber security standards and IT management in a California community college, or other public sector institution.

ABILITY TO:

1. Train, supervise and evaluate the performance of assigned staff.
2. Provide leadership and technical guidance to the District on technology asset security issues.
3. Plan, lead, coordinate and conduct major projects or phases of projects.
4. Apply independent technical judgment to complex technical situations.
5. Coordinate resources with staff, risk management, campus management, and District Police to respond to security breaches.
6. Diagnose and quickly respond to and resolve security breaches and understand reasons for systems failures.
7. Maintain current knowledge of technological advances in the security and related fields.
8. Demonstrate sensitivity to, and respect for, a diverse population.
9. Communicate effectively both orally and in writing.
10. Interpret, apply and explain rules, regulations, policies and procedures.
11. Establish and maintain cooperative and effective working relationships with others.

MINIMUM QUALIFICATIONS:

Candidates/incumbents must meet the minimum qualifications as detailed below, or file for equivalency. Equivalency decisions are made on the basis of a combination of education and experience that would likely provide the required knowledge and abilities. If requesting consideration on the basis of equivalency, an Equivalency Application is required at the time of interest in a position (equivalency decisions are made by Human Resources, in coordination with the department where the vacancy exists, if needed.)

Education:
Bachelor's degree in computer science, management information systems or related field from a regionally accredited institution.

Experience:
Increasingly responsible (2 – 4 years of full time or part time equivalent) experience in data/telecommunications infrastructure, network management and network security, information systems security, including experience with WAN and LAN technologies. Current Cisco security certification or equivalent (e.g., Certified Ethical Hacker (CEH), Certified Information Security Professional (CISSP) or Certified Information Security Manager (CISM)).

Preferred Experience:
Experience in administration

SPECIAL REQUIREMENTS:

Must be able to work occasional evening hours and weekends.