SANTA ROSA
JUNIOR COLLEGE

TITLE: Police Systems Administrator

CLASSIFICATION: Classified

SALARY GRADE: P

JOB DESCRIPTION:

Under general supervision, coordinates the development, maintenance, and administration of the District's law enforcement information and access control systems, services and their infrastructure; maintains law enforcement related electronic devices, equipment associated with the access control system, and the hardware and software which enables the District's connection to the California Law Enforcement Telecommunications System (CLETS); coordinates and performs upgrades, and troubleshooting of hardware/software; addresses security threats; provides specialized technical and training advice to end-users; serves as a lead worker to other classified staff in the area.

DISTINGUISHING CHARACTERISTICS:

The Police Systems Administrator is distinguished from the Systems Administrator by the specialized knowledge of law enforcement procedures and systems, and knowledge of security management systems. The incumbent is required to maintain a POST background clearance in order to complete essential duties and is required to maintain confidentiality of CLETS/CJIS information and systems. The incumbent serves as the primary technical and security contact at SRJC for all county, state and federal law enforcement agencies.

SCOPE:

The Police Systems Administrator develops and maintains overall functionality, security, and ensures uninterrupted availability of the District's law enforcement information and access control systems and services; establishes and maintains user accounts for law enforcement staff for District, County, State and Federal law enforcement systems; and maintains related server infrastructure and related hardware and software.

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. Configures, tests and maintains network, server, workstation and mobile hardware and software which enables access to state and federal law enforcement information systems including Sonoma County Law Enforcement Consortium (SCLEC) systems and services as well as Internet-based law enforcement systems; maintains and updates the SCLEC CAD databases, user accounts, and settings related to buildings and properties in the District's jurisdiction.

2. Identifies and troubleshoots technology-related incidents for software and services; resolves issues and reports to Information Technology Department, if needed.

3. Coordinates and/or performs repair of all hardware, software, peripherals and devices with District staff and third-party vendors; performs follow-up work and ensures timely completion of such repairs.

4. Develops, maintains and deploys hard drive images for hardware/device configurations utilized by the department; develops and maintains documentation of system standards and installation and configuration procedures.

5. Maintains inventory of all technology and communications radios in use by the department; updates and maintains related databases.

KEY DUTIES AND RESPONSIBILITIES – Continued

6. Configures and maintains access control system (C-CURE 9000) consisting of alarm, intrusion detection, and alarm annunciation devices, various sensors, closed circuit television cameras (CCTV), emergency call boxes, and related software; independently operates, troubleshoots, and performs minor repairs.

7. Participates with District staff to coordinate projects related to the access control and CCTV systems; ensures that the scope of work in all bids/quotes comply with District standards and specifications, and existing systems and equipment.

8. Serves as the Agency CLETS Coordinator (ACC) and Security Point of Contact (SPOC) on matters pertaining to the use of CLETS; maintains training and testing records for District Staff as required by DOJ/CLETS policies; prepares responses to various audits performed by the California Department of Justice (DOJ) and the Federal Bureau of Investigations (FBI); serves as the agency technical lead and confidential representative for the SCLEC.

9. Monitors, analyzes, and responds to security threats to District's law enforcement information systems, access control system, surveillance system, network devices, and related servers, workstation and mobile hardware and software.

10. Establishes and maintains user accounts and passwords for all law enforcement information systems, access control and surveillance systems; configures cardholders and issues access cards for the District's access control system.

11. Works with District faculty and staff to ensure proper programming of automated access control schedules.

12. Trains and provides support to end-users in the use of law enforcement information systems, the access control system, the surveillance system, and related components.

13. Assists with designing, editing and maintaining web pages.

14. May oversee special projects or training relevant to job description and act as a representative of the District Police Department.

ABILITY TO:

Work independently; analyze, troubleshoot and maintain network security equipment, law enforcement information systems, access control systems, surveillance systems, network devices, and related servers and workstation hardware and software; work effectively with technical and non-technical users; work effectively and remain calm, under stress in emergency situations; give and follow oral and written instructions; apply standard procedures regarding the use of police radios and department telephones; operate a vehicle in a safe manner; maintain cooperative working relationships; maintain current knowledge of emerging information technology trends and developments; implement new hardware and software solutions; demonstrate sensitivity to, and respect for, a diverse population.

KNOWLEDGE OF:

Principles, practices, and technologies of computer operations and systems analysis; recent Windows and Windows Server operating systems and Active Directory and group policy; Cisco network devices (routers, switches, firewalls), Networking fundamentals: TCP/IP, Wireless, DHCP, DNS; Federal and State Law Enforcement Telecommunications Systems policies and procedures; communications transmitters and receivers and associated systems; website design and development; dispatch radio codes and procedures; electronic systems such as computer-aided dispatch and access control systems; and basic provisions of the California penal and vehicle codes.

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:

Associate's degree in Computer Studies or a closely related field and relevant industry recognized professional certification. Bachelor's degree in Computer Studies or a closely related field and coursework in Administration of Justice preferred.

EXPERIENCE:

Increasingly responsible (2-4 years full-time equivalent experience) recent experience in systems administration and in providing specialized technical server and desktop support (experience with current versions of Microsoft Windows and Windows Server operating systems and Active Directory/corporate domains preferred).

LICENSE OR CERTIFICATE:

- Must possess a valid (Class C) California driver's license and an acceptable driving record.
- Must obtain appropriate Systems Manager and/or Installer/Integrator certification for District's Access Control System within 6 months of hire.
- Must obtain current First Aid and CPR certification within 12 months of hire.
- Must obtain CLETS Train the Trainer Certificate within 12 months of hire.

SPECIAL REQUIREMENTS:

- Must be able to sit for a prolonged period of time in front of a computer monitor.
- Must be able to perform full range of motion activities, such as, but not limited to, walking, standing, lifting (up to 50 lbs. unassisted), or climbing while performing duties.
- Must satisfactorily complete a background investigation, which includes a polygraph, a medical examination, and a psychological examination.
- Occasionally required to work under inclement weather conditions.
- Due to the unpredictable nature of emergency work, the incumbent may occasionally be assigned to work various shifts, including evenings, weekends, and graveyard shifts and holidays.
- Occasional exposure to situations which may be dangerous or life threatening.