

TITLE: Systems Administrator/Security & Access Control

CLASSIFICATION: Classified

SALARY GRADE: C12

SCOPE OF POSITION:

Under general supervision, maintains and administers the District's security and access control systems, services and their infrastructure overseen by District Police to ensure overall functionality, security and uninterrupted availability of the systems; maintains security and access control electronic devices and other equipment associated with the access control system, and the hardware and software which enables the District's connection to the C-CCURE Building Management System; coordinates and performs upgrades, and troubleshooting of hardware/software; addresses security threats; provides specialized technical and training advice to end-users and establishes and maintains user accounts for District staff; serves as a lead worker to other classified employees in the area.

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 and maintains the security and access control system (such as C-CURE) consisting of alarm, intrusion detection, and alarm annunciation devices, various sensors, closed circuit television cameras (CCTV), emergency call boxes, and related software; operates, troubleshoots, and performs minor repairs.
2. Participates with District staff to coordinate projects related to the security, 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.
3. Monitors, analyzes, and responds to security threats to District's security and access control system, surveillance system, network devices, and related servers, workstation and mobile hardware and software.
4. Organizes District facility schedules based on data received from the student information system, the event management system and from District staff. Works with District faculty and staff to ensure proper programming of and updates to automated access control schedules.
5. Maintains inventory of security and access control system technologies.
6. Establishes and maintains user accounts and passwords for all access control and surveillance systems; configures cardholders and issues access cards for the District's security and access control system; updates and maintains related databases.
7. Trains and provides support to end-users in the use of access control and surveillance systems, and related components.
8. Identifies and troubleshoots technology-related incidents for software and services related to the District's access control and security system; resolves issues and reports to Information Technology.

KNOWLEDGE OF:

1. Principles, practices, and technologies of computer operations and systems analysis.
2. Recent Windows and Windows Server operating systems and Active Directory and group policy.
3. Cisco network devices (routers, switches, firewalls).

TITLE: Systems Administrator, Security Access and Control

KNOWLEDGE OF – Continued

4. Networking fundamentals such as TCP/IP, Wireless, DHCP, DNS, use of server and desktop computers and network hardware and software.
5. Emerging information technology trends and developments.
6. Website design and development; internet resources such as web pages and electronic mail.

ABILITY TO:

1. Work independently.
2. Analyze, troubleshoot and maintain network security equipment, security systems, access control systems, surveillance systems, network devices, and related servers and workstation hardware and software.
3. Collaborate productively and cooperatively with technical and non-technical individuals and groups both internally and/or externally.
4. Work effectively and remain calm under stress in emergency situations.
5. Exercise appropriate judgement in interactions with others and with work processes.
6. Communicate effectively, both orally and in writing.
7. Operate a vehicle in a safe manner.
8. Demonstrate sensitivity to, and respect for, a diverse population.

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 the supervising administrators, in coordination with the department where the vacancy exists, if needed.)

EDUCATION:

Associate degree in computer studies or a closely related field and relevant industry recognized professional certification.

EXPERIENCE:

3+ years full-time equivalent recent experience in systems administration and in providing specialized technical server and desktop support, including experience with current versions of Microsoft Windows and Windows Server operating systems.

OTHER REQUIREMENTS:

- 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 security and access control system within 1 year of hire.
- 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.
- Occasionally required to work under inclement weather conditions.
- Must satisfactorily complete a background investigation, which includes a polygraph.

SANTA ROSA JUNIOR COLLEGE COMMITMENT:

All classifications require a commitment to the District's Vision, Mission, Values, Goals and Objectives as articulated in the [Strategic Plan](#).