COMPTON COMMUNITY COLLEGE DISTRICT

CYBERSECURITY - NETWORK SPECIALIST

FLSA: EXEMPT
RANGE 37

DEFINITION

Under the direction of the Chief Technology Officer, the Cybersecurity - Network Specialist designs, implements, and supports the security and infrastructure of systems, servers, peripherals, and network devices. The Cybersecurity Network Specialist also analyzes, plans, designs, implements, maintains, troubleshoots and enhances large complex systems and networks security systems, processes, and policies (including but not limited to server virtualization, LANs, WANs, wireless technologies, and the physical and logical components that integrate these systems together as an enterprise networking backbone).

Incumbents serve as a senior technical architect and systems integrator for large complex systems or networks and are responsible for engineering and supporting standardized solutions that are reliable, scalable, manageable, secure and accessible.

Employees in this classification monitor the work outcomes of other technical staff. This position serves as the lead technical person in a work unit and provides consultation to other IT job classifications. Employees in this classification work with limited supervision within a framework of standard policies and procedures.

SUPERVISION RECEIVED AND EXERCISED

Receives general supervision from assigned management or supervisory staff. Exercises no supervision of staff.

CLASS CHARACTERISTICS

This classification is assigned to the Information Technology Services (ITS) Department and responsible for designing, planning, implementing, and maintaining the District's computer network and server infrastructure, including hardware installation, software installation and configuration, user administration and maintenance, needs analysis, evaluation of vendor hardware/software capabilities, recommending appropriate systems for purchase, troubleshooting, and monitoring operations. Responsibilities include performing diverse, specialized, and complex work involving significant accountability and decision-making responsibility. Successful performance of the work requires skill in managing projects and coordinating assigned work with other District departments, vendors, and contractors. This class is distinguished from Information Technology/Management Information Systems Manager by the latter's full management and supervisory authority in planning, organizing, and directing the full scope of operations within the department.

EXAMPLES OF ESSENTIAL FUNCTIONS (Illustrative Only)

Management reserves the right to add, modify, change, or rescind the work assignments of different positions and to make reasonable accommodations so that qualified employees can perform the essential functions of the job.

- Design, manage, and maintain the District's Network architecture
- Assist in the creation of security policies and procedures.
- Assist with ensuring security policies are applied correctly and meet current requirements.
- Assist in the creation of security training.
- Manage and maintain the District's network authentication systems for wired and wireless network access.
- Manage security policies on firewalls.
- Manage and maintain the District's security event and information system (SEIM).
- Manage and maintain the District's data loss prevention software.
- Manage security policies in Microsoft 365 environment.
- Manage email security system and policies.
- Manage security polices for servers and ensure those policies are applied appropriately and meet current requirements.
- Work with all areas of the IT department to ensure appropriate security policies are implemented.
- Respond to any cyber incidents or events that occur in accordance with the District's incident response plan.
- Design, plan, test, implement, and document complex security enhancements and additions to the network infrastructure.
- Contribute to the design and implementation of the District user directory services.
- Provide high level support of the District's technology infrastructure including but not limited to firewalls, backup, and disaster recovery systems.
- Perform security upgrades on the District's critical IT infrastructure.
- Recommend and implement security policies, protocols, and practices and provide training and guidance to staff.
- Provide guidance, leadership and mentoring to Systems Engineers and other IT staff.
- Support and develop the technical expertise needed to meet long-term business needs.
- Coordinate projects and work activities between operations, applications and systems staff.
- Implement system software/hardware standards, upgrade procedures, and maintenance activities to meet reliability, security, and accessibility standards and expectations for network systems and servers.
- Develop system, hardware, and cost requirements and proposed time frames.
- Troubleshoot network hardware and operating problems, including but not limited to connectivity, internet access, e-mail and servers.
- Develop and maintain complete and accurate records pertaining to hardware, software, system, and network configurations, changes, outages, and improvement plans.
- Compile data and perform analysis as directed.
- Maintain currency with advances in security standards and best practices and recommend new technologies and/or upgrades to current technologies to improve security.
- Work collaboratively and cooperatively with all levels of faculty, staff, and student workers.
- Monitor the work outcomes of other technical support staff and provide performance feedback to supervisors.
- Provide assistance and counsel to faculty and staff pertaining to their computing needs.
- Maintain inventory and related records of network and server hardware, software and licensing.
- Maintain logs and records of work performed.
- Participate in establishing and updating network computing standards, policies, procedures, and use guidelines.

- Perform other related duties similar to the above in scope and function as required.

QUALIFICATIONS

Knowledge of:

- Current NIST, CISO, and A5 standards.
- Incident response best practices.
- Microsoft Active Directory and Azure Active Directory.
- Operating principles and characteristics of LAN/WAN, telecommunications, Wi-Fi, client server environments, and personal computing hardware utilized by the District.
- Current server virtualization, network switching and routing, firewalls, data backup and recovery solutions, cloud computing resources, VoIP systems, business software applications (IE: Office 365), and related systems used by the District.
- Troubleshooting tools for computing hardware and servers, and network equipment including but not limited to switches, routers, and firewalls.
- Advanced level knowledge of desktop and server operating systems including Windows and Linux.
- Methods and procedures of standardizing, securing, maintaining, and operating computing hardware and peripheral equipment in an enterprise environment.
- Software License compliance laws and methods.
- Security and business continuity (disaster recovery and backup) planning and execution.
- Troubleshooting, diagnostic techniques, procedures, equipment and tools used in computing hardware and peripheral repair.
- Technology documentation and presentation techniques.
- Project management methods and techniques.
- Diverse academic, socioeconomic, cultural, disability, and ethnic backgrounds of community college staff and students.

Ability to:

- Apply current NIST and CISO standards to current operations.
- Respond to incidents and events.
- Plan, schedule and perform complex maintenance and upgrades to critical infrastructure.
- Maintain current knowledge of technical advances in all areas of responsibility.
- Prepare clear, concise, and accurate system documentation and reports.
- Establish and maintain cooperative and effective working relationships with others, including those from diverse academic socioeconomic, cultural, ethnic, and ability backgrounds.
- Analyze networking systems and problems, modify current standards, and develop new solutions as required to address changing conditions.
- Analyze network and telecommunication system requirements and select appropriate hardware and software solutions.
- Work independently and exercise sound judgment while meeting schedules and timelines.
- Effectively communicate, orally and in writing.
- Demonstrate interpersonal skills using tact, patience, and courtesy.
- Understand and carry out oral and written directions.
- Monitor the work outcomes of other technical support employees and provide constructive feedback.
- Demonstrated sensitivity to, and understanding of, the diverse academic, socioeconomic, cultural, and ethnic backgrounds of staff and students, as well as staff members and students with physical and/or learning disabilities.

Education and Experience:
Any combination of training and experience that would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

- Associates Degree with coursework in cybersecurity, computer and network systems and technologi computer science, computer engineering, information technology, or an equivalent combination education and experience.
- Demonstrated sensitivity to, and understanding of, the diverse academic, socioeconomic, cultural, a ethnic backgrounds of staff and students, as well as staff members and students with physical and learning impairments.

Preferred Qualifications

- Bachelor's Degree in Cybersecurity, Computer Science, Information Technology, or a related discipline. Relevant industry certifications and training preferred.
- Five years of professional experience with progressively increasing responsibilities and technical expertise in an Information Technology related field.

Other Preferred Qualifications:

- Relevant industry certifications and training (E.G. Cisco Certified Networking Associate, CCNA).

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and to visit various District sites; vision to read printed materials and a computer screen; and hearing and speech to communicate in person and over the telephone. This is primarily a sedentary office classification although standing in and walking between work areas is frequently required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification frequently bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, push, and pull materials and objects weighing up to 50 pounds.

ENVIRONMENTAL ELEMENTS

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees may interact with upset staff and/or public and private representatives in interpreting and enforcing departmental policies and procedures.