SANTA CRUZ COUNTY OFFICE OF EDUCATION

TECHNOLOGY SECURITY AND SYSTEMS ADMINISTRATOR

DEFINITION

Under direction of the assigned administrator, the Technology Security and Systems Administrator independently is responsible for managing and securing the IT infrastructure of the Santa Cruz County Office of Education (COE) and its partner school districts. This role ensures the integrity, availability, and security of network systems, servers, and end-user devices while implementing best practices in cybersecurity, compliance, and IT operations. Guide, support, coordinate and train other Technology Department team members. This position also provides leadership in systems administration, security administration, and help desk & deployment support, ensuring Santa Cruz COE's IT infrastructure remains secure, resilient, and responsive to organizational needs.

SUPERVISION EXERCISED

Provides technical oversight and mentorship to lower-level Technology Department staff, including Help Desk and IT support personnel.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES

Systems Administration:

Manage the installation, configuration and administration of multiple computing and communications systems. Provide ongoing systems administration and maintenance of core services such as email, databases, file IT infrastructure, including servers and telecommunications, web filters and firewalls cloud services, authentication systems, and databases.

Provide support to assigned administrator on projects. Perform project management and oversight, job and equipment specification, documentation, verification, testing and end user interaction with guidance of and reporting to the assigned administrator. Work independently to bring projects to successful completion in a timely and efficient manner.

Prepare project proposals for the assigned administrator's review and approval based upon specifications from end users and departmental needs and managerial guidance. Proposals may include system requirements, definitions, statements of issue, problems and proposed solutions, timelines, pricing, implementation plans and scope.

Explore and make recommendations to the assigned administrator regarding equipment, systems and site specifications, configurations and standards. Ensure each implementation's compatibility and compliance with projects, site and equipment standards. Document Santa Cruz COE IT standards and best practices.

Work to implement and realize the vision and goals of Santa Cruz COE information technology infrastructure and the network services group organization as directed and envisioned by the assigned administrator.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES (CONTINUED)

Troubleshoot hardware, software, and network connectivity problems in a multi-platform, multi-protocol environment. Monitor the status of the network and respond to problems as required.

Serve as an organizational and technical resource to the Technology Support Specialists and Technology Support Technicians for the purpose of guiding and enhancing their professional skills and team cross-functioning.

Provide assistance and training to users on the use of Santa Cruz COE's technology environment.

Document procedures, standards and technical information for the operation. Train, monitor and guide other technicians in the proper and effective use of these procedures, practices and standards.

Maintain and monitor virtualized environments, backup systems, and disaster recovery solutions.

Perform system upgrades, patching, and performance tuning to ensure optimal functionality.

Implement automation and scripting solutions to streamline IT operations.

Maintain accurate documentation of IT procedures, configurations, and workflows.

Lead identify management and directory services architecture.

Security Administration:

Develop, implement, and enforce cybersecurity policies and best practices.

Monitor and manage firewalls, intrusion detection systems, endpoint protection, and data encryption solutions.

Conduct security audits, risk assessments, and penetration testing to identify vulnerabilities.

Ensure compliance with FERPA, CCPA, and other data protection regulations.

Respond to cybersecurity incidents, conduct forensic analysis, and implement remediation strategies.

Serve as the lead trainer for staff cybersecurity awareness programs, reducing security risks through education.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES (CONTINUED)

Help Desk and Deployment Administration:

Oversee Help Desk operations, ensuring efficient issue resolution, ticket management, and support workflows.

Lead all end-user device provisioning and deployment, including MDM configuration and automation.

Manage asset tracking systems, ensuring accurate device inventory and compliance with IT policies.

Establish IT support documentation, training resources, and knowledge bases for Help Desk technicians.

Monitor service requests, user support trends, and system performance metrics to improve response times.

Perform related duties and responsibilities as assigned.

JOB RELATED AND ESSENTIAL QUALIFICATIONS

Knowledge of:

Systems administration, including Windows Server, active directory, Entra/Azure, Linux, and cloud/Mobile Device management environments.

Cybersecurity frameworks (NIST, CIS, ISO 27001) and security best practices.

Network security technologies, including VLANs, VPNs, firewalls, endpoint protection and authentication protocols.

Standard diagnostic and troubleshooting techniques and utilities.

Effective customer service techniques.

Help Desk management tools, IT asset management, and mobile device deployment (MDM solutions such as Jamf, Intune, or Meraki).

Scripting and automation using PowerShell, Bash, or Python for systems administration.

Incident response and forensic analysis for security threats.

Compliance and regulatory requirements for educational institutions.

Knowledge of (continued):
Network standards and communication protocols including TCP/IP, DHCP, OSPF, SMB. CIFS, and DNS.

Scripting and automation to support identity management and device enrollment and processes for device/user profiles.

Skill and Ability to:
Communicate clearly and concisely, both orally and in writing.

Work under limited supervision within a broad framework of standard policies and procedures.

Exercise good judgment, flexibility, creativity, and sensitivity in response to changing situations and needs.

Design, implement, and manage IT infrastructure in collaboration with the Network and Systems Architect while maintaining high availability and security.

Analyze and troubleshoot complex IT issues, identifying root causes and solutions.

Co-lead IT security initiatives, in collaboration with the Network and Systems Architect and other senior staff, proactively mitigating risks and ensuring compliance

Train and mentor staff on cybersecurity and IT best practices.

Effectively communicate technical concepts to both technical and non-technical audiences.

Manage multiple projects and priorities while meeting deadlines.

Identify and coordinate with vendors for the pricing and purchasing of equipment and maintenance contracts. Maintain and renew vendor maintenance and support contracts. Assist in the identification and acquisition of networking, data center and server equipment.

Project manage vendors and partners to support comprehensive installations and deployments
Work after hours/flex time for maintenance windows as needed.

Be courteous and maintain a neat and clean appearance, and demeanor at all times.

EDUCATION AND EXPERIENCE

Any combination equivalent to experience and training that would provide the required knowledge, skills, and abilities would be qualifying. A typical way to obtain the knowledge, skills, and abilities would be:

Education:

Training equivalent to a Bachelor's Degree Information Systems, Cybersecurity, Computer Science, or a closely related field.

Experience:

Minimum of five years of experience in systems administration, security administration, and IT support.

License or Certificate:

Possess specialized training and certification in information systems technology: specific certifications desired include Certified Informations Systems Security Professional (CISSP), Microsoft Certified Azure Solutions Architect, CompTIA Security+, Apple Certified Support Professional (ACSP) or JAMF Certified Tech, Cisco Certified Network Associate (CCNA), and Cisco Certified Network Professional.

Possession of, or ability to obtain, a valid California driver's license and appropriate vehicle operation insurance.

Qualification Requirements

To perform a job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed in the job description are representative of the knowledge, skills, and abilities required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

SPECIAL REQUIREMENTS

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. Essential duties require the following physical skills and work environment:

Ability to travel to different sites and locations with own vehicle (eligible for mileage reimbursement).

While performing the duties of this job, the employee is regularly required to stand and to sit, use hands to finger, handle or feel; reach with hands and arms; stoop, kneel or crouch; talk and hear. Frequently required to walk; occasionally required to move, carry, lift, up to 50 pounds, and occasionally may be required to move, carry or lift up to 70 pounds with assistance.

Occasionally may work in confined spaces and be exposed to dust. Specific vision abilities required by this job include close vision and distance vision.

Approval Date: June, 2012
Revised Date: June, 2018
Revised Date: July 1, 2025 (Previous Title: Technology Infrastructure Analyst)