

INFORMATION TECHNOLOGY ENGINEER IV

NATURE AND VARIETY OF WORK

This is advanced professional and technical engineering work involving creating, implementing, and maintaining the County's enterprise technical infrastructure resources. Incumbents work independently and are responsible for designing, installing, configuring, monitoring, and maintaining network, telecommunications, or systems hardware and software; analyzing hardware and software failures; analyzing connectivity, and monitoring systems and networks to ensure availability to all users; performing necessary maintenance to support network, telecommunications, or systems availability; and developing and implementing information security policies. The incumbent at this level has technical knowledge that is effectively applied to the County's enterprise technical infrastructure in order to handle the more difficult and complex issues involving their specialty area, and/or train/lead lower level subordinates through basic processes.

Work is performed under the supervision of a higher level technology engineer or designated supervisor, and evaluated in terms of technical adequacy, accuracy, and efficiency as evidenced by compliant and proper system and network functioning; and adherence to established timeframes.

EXAMPLES OF WORK (ILLUSTRATIVE ONLY)

Leads subordinate staff in phases of work in their assigned specialty area.

Researches, plans, designs, installs, configures, integrates, monitors, supports, optimizes, and maintains networks, network upgrades, network and server hardware, communication links, and operating systems across the organization.

Ensures the stability and integrity of in-house voice, data, video, and wireless network services.

Administers and maintains end user accounts, permissions, and access rights.

Monitors and tests network performance and provides network performance statistics and reports.

Performs system backups and recovery.

Deploys, integrates, and configures new security solutions and enhancements to existing security solutions in accordance with security procedures.

Recommends additional solutions to existing products to improve overall enterprise security.

Conducts vulnerability audits and assessments, and identifies, investigates, and resolves security breaches detected by in-place security solutions.

Maintains up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes, and the development of new attacks and threat vectors.

Integrates telecommunications systems with enterprise network services and protocols.

Installs, configures, diagnoses, repairs, upgrades, and optimizes telecommunications systems, equipment, facilities, and services.

Designs and supports telecommunications infrastructure and its associated software, including call management systems, voice mail, interactive voice response, and video conferencing systems.

Monitors and identifies capacity and performance issues for telecommunications traffic to ensure continued, uninterrupted operation of telecommunications systems.

Generates telecommunications usage and network traffic reports.

Collaborates in the planning and design of an enterprise Business Continuity Plan and Disaster Recovery Plan.

Writes and implements technical infrastructure policies, standards, baselines, guidelines, and procedures for the assigned specialty area.

Coordinates with equipment vendors during installations and for hardware performance issues to ensure continuity of services.

Resolves second tier end user support issues related to technical infrastructure, such as network access, Internet access, telecommunications, cellular network, servers, viruses, security, hardware, and software.

Willingly and cooperatively performs tasks and duties which may not be specifically listed in the class specification or position description, but which are within the general occupational category and responsibility level typically associated with the employee's class of work.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES

Thorough knowledge of requested specialty area including, but not limited to network and information security, telecommunications, networks, servers, hardware, connectivity, and software applications.

Thorough knowledge of standard computer operating systems.

Thorough knowledge of the county's security goals as established by stated policies, procedures and guidelines and ability to actively work towards upholding those goals.

Thorough knowledge of telephony systems, hardware, and software.

Thorough knowledge of current network hardware, protocols, and Internet standards.

Experience with network design and implementation.

Experience with network capacity planning, network security principles, and general network management best practices.

Hands-on technical knowledge of network and PC operating systems.

Hardware troubleshooting experience.

Experience in the installation, configuration, and optimization of equipment, hardware, and software.

Ability to operate tools, components, peripherals, and testing accessories.

Ability to analyze hardware issues and determine possible solutions.

Ability to communicate effectively, both orally and in writing, with internal and external customers.

Ability to work independently and as a member of a team.

Ability to demonstrate excellence in customer service.

MINIMUM QUALIFICATIONS

Bachelor's degree in computer science, information technology, mathematics, business or public administration, or a closely related field, plus at least three (3) years professional experience in an information technology engineering field, in which at least one (1) year must have involved lead/supervisory duties; or an equivalent combination of education, training, and experience.

CONDITION OF EMPLOYMENT

Must be willing to respond to service calls after normal business hours, when required.

Must have a valid driver's license.