CITY OF MANTECA

IT INFRASTRUCTURE MANAGER

Department: IT & Innovation
Bargaining Group: Mid-Management
Effective Date: August 2025
FLSA Status: Exempt
Revision History:

BASIC FUNCTION:

Under minimal direction of the Director of IT & Innovation or designee, the IT Infrastructure Manager plans, organizes, and manages the City's network, telecommunications, server, and cybersecurity operations. The position is responsible for supervising technical staff engaged in analyzing, planning, implementing, maintaining, troubleshooting, and enhancing large complex systems or networks consisting of a combination that may include personal computers, Virtual Desktop Infrastructure (VDI), cell and mobile devices, switches, routers, firewalls, Local Area Networks (LANs), Wide Area Networks (WANs), point-to-point networks, physical, virtual, and blade servers, Storage Area Networks (SAN), Network Attached Storage (NAS), and the physical and logical components that integrate these systems together as an enterprise networking backbone.

The IT Infrastructure Manager directs staff in planning, managing, and coordinating the day-to-day network operations, maintenance activities, security compliance, and infrastructure projects, including ensuring appropriate training and technical assistance are provided to users as needed. This classification oversees staff responsible for managing infrastructure that supports the Supervisory Control and Data Acquisition (SCADA) systems and may provide assistance in resolving infrastructure issues with these systems when necessary.

The IT Infrastructure Manager also plays a strategic role in developing long-term infrastructure lifecycle plans and capital replacement schedules to ensure the City's enterprise systems remain reliable and cost-effective. The incumbent works with IT & Innovation leadership to recommend citywide technology standards, infrastructure policies, and funding priorities to support critical operations and public safety.

DISTINGUISHING CHARACTERISTICS:

The IT Infrastructure Manager is a mid-management classification responsible for supervising technical staff performing infrastructure and cybersecurity functions. This classification is distinguished by its responsibility for planning, oversight, and coordination of complex enterprise systems rather than daily hands-on troubleshooting.

The incumbent exercises considerable independent judgment in prioritizing projects, allocating resources, and evaluating infrastructure performance, ensuring that staff comply with City policies, industry standards, and security best practices. The position is responsible for developing and recommending citywide infrastructure policies aligned with City goals and advising IT & Innovation leadership on critical infrastructure needs, risks, and funding strategies.

REPRESENTATIVE DUTIES:

ESSENTIAL DUTIES:

Duties may include, but are not limited to, the following. All duties are performed by directing, assigning, and monitoring staff rather than by direct hands-on execution:

- Directs staff in establishing networking environments by installing, configuring, testing, and documenting equipment and network systems according to design and specifications.
- Ensures staff monitor network traffic, analyze server and network activity, and maintain performance monitoring systems, including intrusion detection and virus scanning applications, and appropriate documentation.
- Directs staff performing day-to-day networking tasks to ensure network and server reliability, availability, and serviceability with minimal interruption; ensures staff develop and maintain documentation of area network infrastructure and local and wide area network operations.
- Ensures staff review scheduled system backups; directs troubleshooting of issues as they arise, routine verification of all server backups, and routine backup restore testing; ensures backup configuration of all networking equipment, including switches, firewalls, routers, and other network devices.
- Directs staff assisting department personnel on networking and security troubleshooting; ensures applicable training is provided and advises on information security user training and awareness programs.
-
- Ensures staff maintain inventory records of existing and newly acquired server hardware, software licenses, telecommunications circuits, and network equipment.
- Directs staff in reviewing, maintaining, and implementing network group policies for Active Directory.
- Ensures staff perform security and firmware patching for network equipment, server hardware, and operating systems, following industry recommendations and vendor guidance.
- Directs staff planning, coordinating, configuring, implementing, administering, and maintaining security systems, including firewalls, switches, routers, wireless technologies, physical security for all sites with network access and security systems; ensures proper configuration of network security settings for employees, vendors, and processes for incoming and outgoing internet traffic and internal data flows.
- Oversees staff performing network technology upgrades or expansion, including installation of hardware, software, and integration testing, ensuring security and coordination without impacting existing systems and networks; ensures redundancy plans are tested and documented, backups of all network equipment configurations are maintained, and disaster recovery tests occur at least annually.
- Directs staff developing and maintaining documentation of network topology and troubleshooting of networking hardware and software; ensures accurate planning and coordination for installation, monitoring, and troubleshooting of networks.
- Ensures staff comply with Federal, State, and City laws, codes, ordinances, policies, and procedures relevant to information technology; reviews and approves staff compliance documentation, including FCC licensing for wireless backhaul as required.
- Oversees staff ensuring compliance with PCI requirements; ensures secure electronic payment environments are maintained and appropriate tools are implemented.
- Directs staff setting up, tracking, and troubleshooting all analog and VOIP lines.
- Ensures staff configure, deploy, maintain, and troubleshoot multifactor authentication and VPN software.

- Directs staff designing, implementing, maintaining, and operating information system security controls and countermeasures; assigns project leads for fiber and wiring installations for networking and telecommunications in new buildings or remodels.
- Ensures staff analyze and recommend security controls and procedures in business processes related to information systems and assets; monitors compliance.
- Directs staff monitoring information systems for security incidents and vulnerabilities; ensures monitoring and visibility capabilities are developed and reports on incidents, vulnerabilities, and trends are reviewed and acted upon.
- Directs staff responding to information system security incidents, including investigation of, countermeasures to, and recovery from computer-based attacks, unauthorized access, and policy breaches; ensures staff interact and coordinate with third-party incident responders, including law enforcement; directs staff monitoring for security risks and threats and overseeing implementation of recommendations.
- Ensures staff administer authentication and access controls, including provisioning, changes, and de-provisioning of user and system accounts, security/access roles, and access permissions.
- Directs staff analyzing trends, news, and changes in threat and compliance environments; ensures risk and compliance self-assessments and mitigation plans are conducted and coordinates third-party risk and compliance assessments.
- Oversees staff developing information security governance, including organizational policies, procedures, standards, baselines, and guidelines for information systems and security.
- Ensures staff maintain accurate inventory records of existing and newly acquired networking hardware and software, telecommunications circuits and carriers, servers, security encryption keys, SSL certificates, access points, communications, firmware versions, and network maps.
- Directs staff in maintaining backups of all software programs and retaining accurate electronic historical records, files, and data.
- Develops and recommends long-term infrastructure replacement schedules, technology refresh strategies, and funding priorities to support citywide operations and public safety.
- Oversees the management of vendor coordination, including ensuring vendors and consultants meet all contractual obligations and service expectations.
- Keeps up with regional and state agency initiatives on cybersecurity and critical infrastructure to ensure the City remains aligned with best practices and requirements for essential services.
- Advises City and IT leadership on infrastructure risks, emerging technology trends, and strategic investments critical to maintaining business continuity and citywide service delivery.

OTHER DUTIES:

Create and implement machine policies that align with business policies and procedures.

Conduct user training as needed.

Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

- Supervisory principles, including staff scheduling, training, coaching, and performance evaluation.
- Principles of and current trends in information technology design and implementation across all platforms from endpoints and servers.
- Multiple operating systems, programming languages and tools.
- Network architecture and design fundamentals.
- Wide area network and local area network architecture and infrastructure; networking fundamentals, technologies and protocols.
- Backup and recovery methods.
- Fiber optics, wiring capacities/limitations and LAN and WAN technologies.
- Software development methodologies and life cycles.
- Disaster planning and recovery techniques, debugging and error detection, design and testing tools.
- Principles and practices of project management.
- Mobile data information management.
- Methods of long-term strategic technical planning.
- Principles of documentation and report preparation.
- Pertinent federal, state, and local laws, codes, and regulations.
- General knowledge of SCADA Systems and its infrastructure.
- General knowledge of public safety radio systems and its infrastructure.
- Infrastructure asset lifecycle management and capital improvement planning.
- Emergency management coordination and continuity of operations planning for critical infrastructure.

ABILITY TO:

- Perform a variety of professional, technical, and system programming and/or systems administration duties.
- Use various operating systems and platforms that manage system resources.
- Install, troubleshoot, and program operating systems.
- Problem-solve beyond an intermediate technical level.
- Recommend and implement goals, objectives, policies, and procedures for providing information technology services.
- Understand the organization and operation of the City and of outside agencies as necessary to assume assigned responsibilities.
- Understand, interpret, and apply general and specific administrative and departmental policies and procedures as well as applicable federal, state, and local policies, laws, and regulations.
- Participate in the preparation and administration of assigned budgets.
- Plan and organize work to meet changing priorities and deadlines.
- Work cooperatively with other departments, City officials, and outside agencies.
- Respond tactfully, clearly, concisely, and appropriately to inquiries from the public, City staff, or other agencies on sensitive issues in the area of responsibility.
- Conduct and direct research into information technology issues and products.
- Make group presentations.
- Understand, identify and resolve safety issues and other operational needs.
- Build consensus to bring successful conclusion to various projects and issues.
- Interpret and explain information technology policies and procedures.
- Prepare clear and concise reports.

- Operate office equipment including computers and supporting word processing, spreadsheet, and database applications.
- Communicate clearly and concisely, both orally and in writing.
- Establish and maintain effective working relationships with those contacted in the course of work.
- Work with 3rd party vendors, such as SCADA and public safety radio vendors, to troubleshoot infrastructure issues, as needed
- Learn and observe all appropriate safety precautions as required by the City including, but not limited to, Cal/OSHA General Industry Safety Orders, and City's safety directives.
- Advise IT & Innovation leadership on infrastructure strategies, risks, and funding priorities.

EDUCATION AND EXPERIENCE:

Any combination of training and experience which would provide the required knowledge and skill. A typical way to obtain the required knowledge and skill would be:

Education: A Bachelor's degree from an accredited college or university with major course work in computer science, information systems, or a related field.

Experience: Five (5) years of increasingly responsible professional information technology experience.

OR

Education: Equivalent to an Associate's degree from an accredited college or university with coursework in Computer Science, Management Information Systems or closely related field.

Experience: Seven(7) years of increasingly responsible professional information technology experience.

OR

Experience: Nine (9) years of increasingly responsible professional information technology experience.

AND

At least one (1) year of the above experience must have been in a supervisory, senior, or lead capacity. Experience with supporting SCADA and public safety systems is preferred.

Preferred Experience:

- Hands-on networking experience, systems administration or operating system programming in a multi-platform, large scale application and operating system environment. Prior experience must include testing, installation, documentation, and maintenance of system software and hardware/network configurations.
- Experience with Windows, Linux, macOS, Active Directory, Microsoft Office, Microsoft 365, Microsoft Exchange, and SQL is required.
- Experience with VMware, ERP systems, Backup, VOIP, Helpdesk software, Firewalls, Virtual Private Network (VPN), Multifactor Authentication, and L2/L3 network switches experience

is desirable.
- Experience in Hyper Converged Infrastructure (HCI).
- Experience in scripting (PowerShell, Python, Perl, etc.) for task automation.
- Familiarity with cloud technologies.
- Experience with directory services.
- Experience developing and implementing infrastructure lifecycle plans and capital improvement schedules.
- Experience overseeing the management of vendor coordination, including ensuring vendors fulfill all contractual duties and service expectations.
- Experience advising IT leadership on strategic technology initiatives and infrastructure funding priorities.

LICENSES AND OTHER REQUIREMENTS:

Possess a valid California Class C driver's license.

Willingness and ability to work the hours necessary to accomplish the assigned duties, including before and after normal work hours; be available for technical support and emergencies; attend meetings, seminars, conferences, and training classes during work and non-work hours; travel out of town and/or out of state for several days at a time.

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Driving a vehicle to conduct work.
Indoor & outdoor work environment.
Subject to noise from equipment operation.
Emergency callouts.
Seasonal heat and cold or adverse weather conditions.

PHYSICAL DEMANDS:
Dexterity of hands and fingers to operate a computer keyboard.
Hearing and speaking to exchange information.
Sitting for extended periods of time.
Bending at the waist, kneeling or crouching to reach computer equipment.
Seeing to view a computer monitor.
Lifting and carrying moderately heavy computer equipment.

HAZARDS:
Exposure to chemical fumes and odors.
Working around and with machinery having moving parts.