

CITY OF CHATTANOOGA

Classification Specification Title: Director Infrastructure, Security, and Camera Operations

Department: Technology Services

Pay Grade: GS. 16

Supervision Received From: Chief Information Officer

FLSA Status: Exempt

Supervisory Responsibility For: Mgr. Camera Systems; Mgr Networking; Mgr Compute & Storage; IT Sec. Analyst; IT

Established: 5/16/25

Revision Dates: None

Sec. Spec., IT Security Intern

CLASSIFICATION SUMMARY:

Incumbent in this classification is a critical leadership position responsible for the strategic planning, development, implementation, and maintenance of the City of Chattanooga's core technology infrastructure, comprehensive cybersecurity systems and city-wide camera operations. Reporting to the Chief Information Officer (CIO), this role requires an experienced leader with a strong technical background, exceptional management skills, and a deep understanding of the evolving landscape of infrastructure, security threats, and public safety camera technologies. The Director will ensure the reliability, security, and efficiency of these vital systems (including related data systems), directly impacting the safety and well-being of Chattanooga residents, businesses, and visitors.

SERIES LEVEL:

The Director Infrastructure, Security, and Camera Operations is a stand-alone position.

ESSENTIAL FUNCTIONS:

(The following duties ARE NOT intended to serve as a comprehensive list of all duties performed by all employees in this classification, only a representative summary of the primary duties and responsibilities. Incumbent(s) may not be required to perform all duties listed and may be required to perform additional, position-specific duties.)

Supervises staff to include prioritizing and assigning work; conducting performance evaluations; ensuring staff are trained; ensuring that employees follow policies and procedures; maintaining a healthy and safe working environment and making hiring, termination and disciplinary recommendations.

Develop and execute a comprehensive strategic plan (short- and long-term) for the City's technology infrastructure (network, servers, data centers, cloud operations), security posture (cybersecurity), and camera operations, aligning with the Department's and City's overall goals and priorities. Create metrics and KPIs that provide actionable insights that support the effective delivery of strategic outcomes and daily operations of this division.

Oversee the city's infrastructure teams to ensure the integrity, security, and efficiency of Chattanooga's enterprise IT environment, operating in accordance with established policies and procedures. This encompasses strategic planning, implementation, and maintenance of IT infrastructure, including data centers, cloud services, network security, and disaster recovery. Ensures the City data center environments are secure and perform within established guidelines in relation to policies and procedures. Lead and oversee the design, implementation, management and maintenance of the city's robust and reliable technology infrastructure to include computing and network infrastructure, data storage solutions, and cloud-based services. Ensure scalability and resilience to support the City's growing needs.

Establish, refine, and enforce cybersecurity policies aligned with federal, state, and local government regulations. Continuously assess cyber threats, respond to incidents, and lead recovery efforts to minimize risks. Conduct security audits and vulnerability analyses on city networks, software applications, and hardware systems. Ensure proper controls are in place for accessing all city systems and applications. Educate city staff on cybersecurity best practices, data protection, and phishing prevention strategies. Work with law enforcement agencies, IT professionals, and regulatory bodies to maintain Chattanooga's cybersecurity integrity, including the integrity of the City's data systems and protected data types (HIPPA, PII, and CJIS). Oversee the selection and deployment of security software, firewalls, encryption tools, and other protective measures. Guide and manage any necessary or requested security-related investigations, including those related to Criminal Justice Systems Information (CJIS). Maintain thorough documentation of cyber incidents, breaches, and mitigation strategies.

Strategically manage the City's network of cameras, delivering the required coverage, functionality, data security, and compliance with relevant regulations and privacy considerations. Explore and implement innovative camera technologies to enhance public safety and operational efficiency. Ensure the camera system is operating reliably 24x7x365, orchestrating monitoring systems to proactively identify issues and the necessary troubleshooting and problem resolution efforts across internal teams, other departments and suppliers of the technology platform. Establish and enforce protocols for the secure storage, retrieval, and dissemination of camera footage, adhering to privacy laws and organizational policies.

Build, mentor, and lead a high-performing team of technical professionals across infrastructure, security, and camera operations. Foster a collaborative and innovative work environment. Develop annual plans and goals for the team. Monitor progress against goals, provide feedback and coaching as required to managers and others on the team. Supervise and review team performance and provide effective coaching and counseling when required. Build and execute annual technical skills training and certification plans for each team member, ensuring completion.

Work with the CIO and other department leaders to develop the annual budgets for infrastructure, security, and camera operations. Ensure cost-effectiveness and responsible resource allocation and use of operating and capital funds. Build and manage relationships with relevant technology vendors, service providers, consultants/contractors, ensuring contract compliance and optimal service delivery. Review financial statements related to division operations and ensure division stays within budget and allocated resources are used efficiently and effectively.

Collaborate effectively with other City departments, external agencies (TBI, FBI, and TN State Comptrollers Office) to ensure seamless work coordination and communication regarding infrastructure, security, and camera initiatives. Work closely with other DTS divisions and city departments to assess technology needs and implement solutions that enhance municipal operations. Collaborate with DTS divisions, city departments, external agencies, contractors, attorneys and/or other interested parties to coordinate activities, review work, exchange information and resolve problems.

Ensure compliance with all applicable federal, state, and local laws, regulations, and standards related to technology infrastructure, security, and data privacy. Identify and mitigate potential risks. Oversees periodic audits of related system usage and connections to ensure compliance with Safeguarding Member Information Standards and Procedures, City policies and to guard against unauthorized users and to prevent the introduction of any undesirable or destructive software. Develop disaster recovery and business continuity plans for critical infrastructure, security, and camera systems.

Continuously monitor emerging trends and advancements in infrastructure, security, and camera technologies relevant to a smart city environment like Chattanooga. Recommend to the CIO which trends and technologies need to be incorporated into annual and multi-year plans.

Participate in meetings, public events, training sessions, committees, and other related events to share and receive information.

Direct, review, and participate in creating various reports, work papers, communications, schedules, and other related documents for internal departments, government entities, external agencies, contractors, and other interested parties.

Use, carry, and answer a cell phone for business purposes as required by job duties and the department head.

Must meet regular attendance requirements.

Must be able to maintain good interpersonal relationships with staff, co-workers, managers and citizens.

Must accomplish the essential functions of the job, with or without reasonable accommodations, in a timely manner.

Performs other duties as assigned.

DEPARTMENT SPECIFIC DUTIES (if any):

MINIMUM QUALIFICATIONS:

Bachelor's degree in Computer Science, Information Technology, Cybersecurity, Engineering, or a related field. Minimum of ten (10) years of progressively responsible experience in managing complex technology infrastructure, security systems, and camera operations, with at least four (4) years in a management leadership role, five (5) years of cybersecurity experience, preferably in government or municipal operations, and five (5) years of experience in IT infrastructure management, preferably within government or large-scale enterprise environments; or any combination of equivalent experience and education. Master's Degree preferred.

LICENSING AND CERTIFICATIONS:

Required: Valid Driver's License

Preferred: Information Technology Management and Leadership Professional (ITMLP); Criminal Justice Information Services awareness training (CJIS); ITIL Certification; CompTIA Certifications (Security+, Network+, Infrastructure+); Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM); VMware Certified Data Center Virtualization (VCTA-DCV); Cisco Certified Network Professional (CCNP); SNIA Certified Storage Networking Expert (SCSN-E) or other Storage Certifications; Google Cloud Associate or Professional; AWS Cloud Practitioner or Solutions Architect; Project Management Professional (PMP); Six Sigma or Lean/SixSigma Green Belt

KNOWLEDGE AND SKILLS:

Knowledge of troubleshooting complex systems and using root cause analysis models and other methods to determine potential solutions quickly and effectively. Knowledge of managerial and leadership principles and practices. Understanding of municipal government or business structures and operations. Knowledge of budgeting principles and practices. Understanding of relevant legal and regulatory requirements related to data privacy and security. Knowledge of advanced financial analysis principles and methods. Strong understanding of customer experience principles and service delivery excellence. Extensive knowledge of network architecture and infrastructure, server administration, system virtualization, cloud computing, and data center operations. Extensive experience with infrastructure governance and ITIL processes. Deep understanding of all cloud operating environments with a focus on AWS and Google. Proven track record of managing cloud migration and standardization initiatives. Extensive knowledge and use of automation tools in an infrastructure operations environment. Deep understanding of cybersecurity principles, frameworks, and best practices, including risk assessment, threat intelligence, and incident response. Familiarity with Tennessee state regulations and federal cybersecurity mandates affecting local governments preferred. Understanding of applicable Federal, State, and Local laws, standards, and procedures.

Mastery of relevant technologies across network, server, storage, and cloud infrastructure. Expert proficiency in infrastructure monitoring and management tools. Expertise in security frameworks such as NIST, ISO 27001, and CIS Controls. Substantial experience in selecting, deploying, operating, and maintaining cybersecurity software. Experience conducting security audits and security-related investigations, either directly or through the selection and use of a qualified supplier, to include CJIS-related investigations. Experience with managing and deploying large-scale camera systems, video management software (VMS), and analytics. Experience with managing, operating, and maintaining VMS systems such as Genetech. Experience with the use of public safety camera systems with a Real Time Information Center. Experience developing and implementing the overall strategy for public safety camera systems. Experience troubleshooting technical issues, managing maintenance schedules, and coordinating repairs. Experience creating and maintaining policies and procedures for camera usage, data access, retention, and compliance. Skill in developing and managing budgets and developing strategic plans. Skill in performing mathematical calculations. Skill in reading, comprehending, and reviewing financial information. Experience managing projects and adapting to a rapidly changing environment.

Ability to make program decisions based on financial considerations. Ability to understand multiple objectives and assess optimal courses of action. Ability to work effectively under pressure and manage multiple priorities. Ability to analyze complex business and technical problems and make appropriate recommendations. Ability to project consequences of proposed actions and make recommendations supporting organizational goals. Ability to handle multiple tasks simultaneously. Ability to prepare and analyze complex financial reports. Proven ability to manage high-performing teams and outsourced vendor relationships. Proven ability to develop and implement strategic technology plans and budgets.

PHYSICAL DEMANDS:

Positions in this class typically require reaching, fingering, grasping, talking, hearing, seeing and repetitive motions.

WORK ENVIRONMENT:

Sedentary Work: Exerting up to 10 pounds of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull or otherwise move objects, including the human body. Sedentary work involves sitting most of the time. Jobs are sedentary if walking and standing are required only occasionally and all other sedentary criteria are met.

SPECIAL REQUIREMENTS:

Safety Sensitive: N

Department of Transportation - CDL: N

Child Sensitive: N

The City of Chattanooga, Tennessee is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the City will provide reasonable accommodations to qualified individuals with disabilities and encourage both prospective and current employees to discuss potential accommodations with the employer.