CITY OF CHATTANOOGA

Classification Specification Title: IT Security Analyst 2

Department: Technology Services	**Pay Grade: GS. 11**
Supervision Received From: Dir. Infra., Sec., & Camera Ops.	**FLSA Status: Exempt**
Supervisory Responsibility For: None	**Established: 6/06/25** **Revision Dates: N/A**

CLASSIFICATION SUMMARY:
Incumbents plan and implement security measures to protect the City's computer systems, networks, and to ensure the confidentiality, integrity, and availability of City data. The IT Security Analyst II performs risk assessments and tests data processing systems. This role creates, tests, and implements network disaster recovery plans. It also involves regularly reviewing logs for breaches or suspicious activity and ensuring that data encryption and other necessary security measures are in place. The IT Security Analyst II is expected to stay current on the latest intelligence, including hackers' methodologies, to anticipate security breaches. This position acts as a forward-thinking innovative security architect that can effectively protect existing networks by researching, identifying, and recommending security enhancements.

SERIES LEVEL:
The IT Security Analyst 2 is the second level of a three-level series.

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.)*

Perform the day-to-day IT security operations of the City's IT Security team including: auditing server and network access, audit server and network equipment patch levels, reviewing logs, documenting vulnerabilities and plan resolution, and ensuring security systems are online and enforced.

Monitor and maintain physical and logical access controls on IT Security equipment and user account policies.

Ensures IT assets are secure.

Gather and analyze information from departments to determine and set disaster recovery operations.

Audit IT security measures and user account access levels to achieve maximum effectiveness of IT systems and users.

Assist and advise the Director of Infrastructure, Security and Camera Operations on matters pertaining to strategic and action plans for IT security, disaster recovery, penetration testing, use policy, IT change management, and other IT security related matters.

Assess potential technical solutions for IT security best practices.

Conduct threat monitoring and analysis using various threat detection, investigation and response (TDIR) capable tools, such as security information and event management (SIEM) and extended detection and response (XDR) platforms.

Conduct multi-telemetry based threat investigations to identify cyber threats coming both internally and externally of the organization.

Triage alerts from detection platforms, identifying and removing false positive issues and escalating genuine identified attacks.

Document formal, technical incident reports for consumption by infrastructure teams and senior leadership.

Provide infrastructure teams with incident support, including mitigating actions to contain activity and advisory for remedial actions.

Work with threat detection content development teams to enhance/tune detection platforms, and create new detection content.

Carry out root cause analysis and investigations to advise on prevention mechanisms and configuration changes.

Work with Threat Intelligence teams to research emerging threats and exploits to aid in the discovery of incidents. Maintains knowledge of latest security technologies and mitigations.

Work with threat hunting teams to optimize TDIR capabilities through threat hunting findings.Supports the development and running of reporting for compliance and infrastructure teams as well as performance reporting for the security operations team.

Carry out analysis and testing for the purposes of identifying vulnerabilities, misconfigurations or other exposures, and the validation of user policies.

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 or equivalent education and work experience with training emphasis in IT Security, Computer Science, Information Systems technology or other closely related field. Minimum of four (4) years of experience in an IT Security role or equivalent with experience in IT audit, network operations, enterprise risk management, penetration testing, red team/incident responder, or as a junior security operations analyst or any combination of equivalent experience and education. Minimum of four (4) years of experience or equivalent with regulatory compliance and information security management frameworks (such as International Organization for Standardization [ISO] 27000, COBIT, National Institute of Standards and Technology [NIST] 800); or any combination of equivalent experience and education.

LICENSING AND CERTIFICATIONS: Preferred

ITIL Certifications

CompTIA Certifications (CompTIA Infrastructure+, CompTIA Networking+, CompTIA Security+)

Project Management Professional (PMP)®

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Auditor (CISA)

Certified Information Security Manager (CISM)

Six Sigma or Lean/SixSigma Green Belt

KNOWLEDGE AND SKILLS:

Knowledge of monitoring security information and event management (SIEM) systems & tools; network and security technologies, such as firewalls, IDS/IPS; configuring and utilizing and vulnerability assessment technologies; monitoring networks, detecting threats, and responding to incidents; report writing, investigational techniques and communicating to large audiences; applicable federal, state and local laws, ordinances, codes, rules, regulations, policies and procedures; policy and procedure development practices; relational database concepts; network principles; applicable operating systems; applicable software products; current technologies; project management principles and practices; organizational mission, values, goals and consistent application of this knowledge.

Ability to establish and maintain effective working relationships with others. Ability to interpret and apply applicable laws, ordinances, codes, rules, regulations, policies and procedures. Ability to resolve the most complex technical support problems.

.

Strong problem-solving, critical thinking, and troubleshooting skills. Skills in decision-making capabilities, with a proven ability to weigh the relative costs and benefits of potential actions. Interpersonal skills as applied to interaction with coworkers, supervisor, and the general public, sufficient to exchange or convey information and to receive work direction.

PHYSICAL DEMANDS:

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

WORK ENVIRONMENT:

Medium Work: Exerting up to 50 pounds of force occasionally, and/or up to 20 pounds of force frequently, and/or up to 10 pounds of force constantly to move objects.

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.