



Job Specification

Job Title: Information Technology Specialist (Information Security Analyst I)	FLSA Type: Exempt	Date Established: 3/25/2025
Department: DoIT	EEO Code: 3	Date Revised:
Class Code: 15112232	Reports To: Cyber Security Supervisor	Date Approved:

Job Summary

Under general supervision of the Cyber Team, the Information Technology Specialist 1 – (Information Security Analyst I) is responsible for preventing data loss and service interruptions by assisting Information Security Analysts and researching new technologies that will effectively protect the City’s IT Infrastructure. Work involves a wide range of functions designed to ensure the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs.

Essential Duties and Responsibilities *(may perform other duties as assigned)*

- Monitor security monitoring tools and information gathering.
- Perform analysis of alerts, logs, security platforms, and systems.
- Assist in Vulnerability Management and Reporting.
- Support incident response and investigations.
- Analyze and interpret policies and guidelines.
- Review violations of computer security procedures and confab with Cyber Team on user corrective action.
- Participate in Cyber Awareness Training.
- Monitor current CVE reports to communicate threat levels to Cyber Team.
- Implement security measures.
- Maintain security posture.
- Evaluate and solve incident response issues.
- Analyze and interpret policies and guidelines.
- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs
- Review violations of computer security procedures and discusses procedures with violators to ensure violations are not repeated
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Perform risk assessments and executes tests of data processing systems to ensure functioning of data processing activities and security measures.
- Confer with users to discuss issues such as computer data access needs, security violations, and programming changes.
- Coordinate implementation of computer system plan with other DoIT personnel, City agencies, and outside vendors.

- Train users and promotes security awareness to ensure system security and to improve server and network efficiency.
- Perform special projects and other duties as assigned.

Qualifications (required):

- Completion of coursework from an institution of higher education in cyber security, computer science, information systems, programming systems analysis or other related field of study
- Associate's or Bachelor's degree in cyber security, computer science, information systems, programming systems analysis, geographic information science, engineering communications or other related field of study
- Minimum of one (1) year of experience implementing or working with vulnerability management

Equivalent combinations of education and experience may be substituted to meet the education and experience requirements of this position.

Qualifications (preferred):

- Foundational certifications such as A+, Net+ and Sec+ are preferred.
- Familiar with Cloud Security concepts and methodologies.
- Understanding of and experience applying security fundamentals.
- Conceptual understanding of security methodologies and challenges.
- Forensics certification or experience with computers.
- Experience in Cyber policy review and education.
- Experience verifying vulnerabilities and weaknesses in system design.
- Experience with IOT Security

Knowledge, Skills, and Abilities

- Knowledge of a wide range of security tools.
- Knowledge of current platform technologies managed by security products (SQL, IIS, Windows, Linux, Mac).
- Ability to learn security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management, etc.
- Ability to produce threat management preparation of reports, dashboards, and documentation.
- Good written and verbal communication skills.
- Good analytical skills, problem solving, and interpersonal skills.
- Ability to work virtually and independently on assignments from supervising team.
- Ability to remain current on the latest threat and technologies.
- Knowledge in one or more of the following: endpoint protection, data loss prevention, SIEM, EDR, vulnerability management, firewall rules management, secure web gateway/ proxy.
- Knowledge of and experience in a wide range of security tools.
- Functional knowledge of current platform technologies managed by security products (SQL, IIS, Windows, Linux, Mac).
- In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management, etc.
- Skill in threat management preparation of reports, dashboards, and documentation.
- Good written and verbal communication skills.
- Good analytical skills, problem solving, and interpersonal skills.
- Ability to work independently or in medium group settings.
- Ability to stay up to date on the latest threat and technologies.
- Ability to effectively interact with other IT Service professionals and non-technical employees.

Licenses, Certifications, and Other Special Requirements:

Candidates considered for placement in this classification may be subject to a Criminal Background Investigation and the execution of an NDA based on the requirements of the position.

Physical Demands

The individual generally remains in a stationary position for an extended period operating standard office equipment, which may include computers, telephones, photocopiers, and fax machines. May be required to lift or be able to lift up to 10 pounds for short period of time.

Work Environment

Work is performed primarily in a virtual environment.

The above statements reflect the general nature and level of work performed by employees assigned to this class. Incumbents may be required to perform job-related responsibilities and tasks other than those stated in this specification. Essential duties may vary from position to position.

Notes: