



Office of Human Resources  
IT Security Analyst Associate – CI3293  
THIS IS A PUBLIC DOCUMENT

### General Statement of Duties

Performs routine professional level information security work enforcing security practices and protocols, which includes monitoring security systems and alerts, and participates in the analysis and evaluation of enterprise information security systems.

### Distinguishing Characteristics

The IT Security Analyst Associate performs routine level information security work enforcing security practices and protocols, which includes monitoring security systems and alerts.

The IT Security Analyst Senior performs full-performance level information security work enforcing security practices and protocols, which includes installing, configuring, and monitoring security systems and alerts, and analyzing and evaluating enterprise security systems.

The IT Security Specialist performs specialized level information security work identifying security issues and risks, ensuring security systems are optimal, resolves complex security systems issues, and may work independently within other divisions of the organization.

The IT Security Manager is responsible for the management and supervision of information technology security personnel engaged in the security of information technology systems throughout the city.

### Essential Duties

Monitors and analyzes security systems and data networks, which include reviewing firewall and router alerts, network device alerts, and monitoring intrusion prevention and detection systems.

Monitors critical information security systems infrastructure for operating errors and risks to systems availability.

Performs Information Security Incident Response and investigation activities and maintains logs to record and report incidents.

Prepares reports on an as needed basis for compliance, change management, systems monitoring, and intrusion analysis.

Participate in all phases of the system development lifecycle as it relates to new information security initiatives and projects. This includes design, testing and modifying new systems, and assisting with enterprise deployments.

Assists with the management of information security services ticket queue and ticket resolution and escalation. Creates changes requests for modifications to security systems such as firewalls, VPNs, access controls, web proxies, login environments, and other security systems.

Performs other related duties as assigned.

Any one position may not include all of the duties listed. However, the allocation of positions will be determined by the amount of time spent in performing the essential duties listed above.

**Competencies**

Analyzing - Analyzes data and all other sources of information, patterns, and relationships. Demonstrates an understanding of how one issue may be a part of a much larger system.

Applies Technology to Tasks - Selects and understands procedures, machines, or tools that will produce the desired results; identifies or solves problems in machines, computers, or other technologies as they are related to performing tasks.

Technical Competence - Uses knowledge that is acquired through formal training or extensive on-the-job experience to perform one's job; works with, understands, and evaluates technical information related to the job; advises others on technical issues.

Technical Problem Solving - Troubleshoots diagnoses, analyzes, and identifies system malfunctions to determine the source and cause of the problem.

**Knowledge & Skills**

Knowledge of information security infrastructure and architecture.

Knowledge of the principles and processes of both tactical and strategic information technology program management.

Knowledge of life cycle and risk management and the mechanisms by which they tie to policy compliance.

**Level of Supervision Exercised**

None

**Education Requirement**

Bachelor's Degree in Computer Science, Information Systems, Business Administration, Mathematics or a related field.

**Experience Requirement**

Two (2) years of administering information security systems to include any or all of the following: information security architecture, information security procedures and controls, physical security, attack & penetration testing, application testing, information assurance program gap analysis and incident response.

**Education & Experience Equivalency**

One (1) year of the appropriate type and level of experience may be substituted for each required year of post-high school education.

Additional appropriate education may be substituted for the minimum experience requirements.

**Licensure & Certification**

None

**Working Environment**

Work is primarily performed in an office setting and frequently at other locations for meetings. Work involves pressure due to multiple calls and inquires and is subject to interruption.

**Level of Physical Demand**

1-Sedentary (0-10 lbs.)

**Physical Demands**

(Physical Demands are a general guide and specific positions will vary based on working conditions, locations, and agency/department needs).

Balancing: Maintaining equilibrium.

Eye/Hand/Foot Coordination: Performing work through using two or more body parts or other devices.

Hearing: Perceiving and comprehending the nature and direction of sounds.

Oral Comprehension: Ability to discern the meaning of oral speech.

Sitting: Remaining in a stationary position.

Talking: Communicating ideas or exchanging information.

Vision Far Acuity: Ability to perceive or detect objects clearly at 20 feet or more.

Vision Near Acuity: Ability to perceive or detect objects at 20 inches or less.

Walking: Ability to move or traverse from one location to another.

Written Comprehension: Ability to discern the meaning of written words.

**Background Check Requirement**

Criminal Check

Education Check

Employment Verification

By position, Motor Vehicle Record

**Assessment Requirement**

None

**Probation Period**

Six (6) months.

**Class Detail**

**Pay Grade: EX-10**

**FLSA Code: Y**

**Established Date: 2/14/2021**

**Established By: JH**

**Revised Date:**

**Revised By:**

**Class History:**

This is a new classification that was developed as part of the IT Security Study 2020.