DENVER
THE MILE HIGH CITY

Office of Human Resources
IT Security Specialist - CI2796

THIS IS A PUBLIC DOCUMENT

General Statement of Duties

Performs specialized professional 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.

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

Designs, configures, and analyzes security systems to ensure the effectiveness and resiliency of information technology systems to cyber threats, and leads the implementation of security projects to ensure proper implementation and optimal configuration.

Analyzes and evaluates all aspects of the enterprise information security system (e.g. information security architecture, disaster plans, etc.), and provides technical knowledge and advice regarding the development and implementation of procedures for maintaining information systems and network technology.

Develops security-based projects, which includes scope and design, definition requirements, procedures, architecture (logical/physical), testing, documentation, and implementation.

Enforces compliance with security policies and procedures to ensure the integrity and protection of information systems and data in accordance with applicable rules, laws, and regulations.

Assesses internally developed security solutions and new technologies for impacts and implications to overall security operations, which includes evaluating the cyber landscape for emerging threats and vulnerabilities.

Conducts and assists with security audits, and provides recommendations to mitigate security risks.

Evaluates security architecture alternatives, which includes mediating opposing viewpoints and negotiating equitable outcomes to ensure sustainable solutions.

Key contributor in security investigations and the Security Incident Management protocol.

Participates in researching current and proposed federal, state, and local laws and regulations, industry trends, and best practices in the field of information security to determine their applicability to information technology security operations.

Drives the development of policies and procedures to maintain consistency across security platforms, and implements changes necessary for compliance with laws, rules, and regulations.

Provides consultation and advice to senior management and other information technology professionals, to include technical and administrative staff throughout the city regarding security issues.

Conducts and assists with security audits and provides recommendations to mitigate security and systems risks.

Documents and diagrams security architecture, to include the realtionships between cyber security systems and other technology platforms.

Performs other related duties as assigned.

Employees may be re-deployed to work in other capacities in their own agencies or in other City agencies to support core functions of the City during a City-wide emergency declared by the Mayor.

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 complex 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

By position, supervises clerical and technical level staff.
By position, matrix manages staff involved with projects or programs.

Education Requirement

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

Experience Requirement

Three (3) 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

By position, must obtain Criminal Justice Information Services (CJIS) clearance within the probationary period.

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
By position, must obtain Criminal Justice Information Services (CJIS) clearance within the probationary period.

Assessment Requirement

None

Probation Period

Six (6) months.

Class Detail

Pay Grade: EX-16
FLSA Code: Y
Established Date: 9/21/2018
Established By: LS
Revised Date: 7/30/2023
Revised By: AM
Class History: 7/30/2023 – Revised licensure & certification and background checks.