DENVER
THE MILE HIGH CITY

Office of Human Resources
IT Security Manager - CI1870

THIS IS A PUBLIC DOCUMENT

General Statement of Duties

Manages an information technology security division, which includes implementing the overall strategic plan to safeguard information technology assets and interests from intentional or unintentional modifications, disclousres, or the destruction and tampering of systems, which includes disaster recovery, database protection, and software development.

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

Manages and oversees an information technology security division and reltated security personnel engaged in enforcing security practices and protocols, which includes installing, configuring, and monitoring security systems and alerts, and analyzing and evaluating enterprise security systems and controls necessary for protecting citywide information technology assets and interests.

Monitors and evaluates cyber security systems and network security practices to ensure compliance with and enforce adherance to citywide policies and procedures with reguard to managing security for all electronic systems and databases.

Researches current and proposed federal and state laws and regulations, industry trends, and best practices in the field of information technology and cyber security to determine their applicability for citywide operations.

Analyzes and evaluates all aspects of enterprise information security (e.g. information security architecture, disaster plans, etc.) then provides guidance on the development and implementation of procedures for maintaining citywide information systems and networks.

Provides consultation and advice to information technology managers and other professionals throughout the city on information technolongy and cyber security issues.

Organizes and applies standards, procedures, systems and guidelines.

Implements policies, programs, operating procedures and practices and effectively manages operating costs, and ensures budget remains at or below established targets.

Coaches, mentors, and challenges staff. Champions continuous improvement, including devising new strategies and new opportunities. Leads staff development initiatives that include training, development, and succession planning.

Develops goals, documents performance, provides performance feedback and formally evaluates the work of the employee; provides reward and recognition for proper and efficient performance. Assists staff to achieve performance standards and identifies opportunities for continual improvement to performance standards.

Fosters an atmosphere of innovation in order to challenge the organization to think creatively, especially as it relates to positive citizen and customer experience opportunities.

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

Delivering Results - Sets high standards for quality, quantity, and timelines. Focuses on customer needs and satisfaction. Consistently achieves project goals.

Influencing - Collaborates with, persuades and influences others.

Coaching - Provides others with clear direction, motivates, and empowers. Recruits staff of a high caliber and provides staff with development opportunities and coaching.

Deciding and Initiating Action - Takes responsibility for actions, projects and people; makes quick, clear decisions which may include tough choices, after considering risks.

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 infrastructures.

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.

Ability to establish formal methodologies and promote best practices on behalf of the City.

Level of Supervision Exercised

Manages a work group within a division by supervising information technology security personnel and/or individual contributors.

Education Requirement

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

Experience Requirement

Three (3) years of professional level information technology experience which included the performance of duties most of the following areas: information security architecture, information security procedures and controls, physical security, attack & penetration testing, application testing, information security 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-18
FLSA Code: Y
Established Date: 9/21/2018
Established By: LS
Revised Date: 7/30/2023
Revised By: AM
Class History: 2/14/21 - The classification was revised and updated with the IT Security Study in 2020.
11/27/2022 - Revised pay grade as a result of CN1746.
7/30/2023 – Revised licensure & certification and background checks.