DENVER
THE MILE HIGH CITY

Office of Human Resources
IT Data Protection Analyst Senior – CI3433

THIS IS A PUBLIC DOCUMENT

General Statement of Duties

Performs full-performance professional level work analyzing the governance of information technology systems from a risk assessment and compliance stance, which includes identifying security vulnerabilities with end-users and applications with a focus on policies and procedures.

Distinguishing Characteristics

The IT Data Protection Analyst Staff performs entry-level work learning and assisting with assessing areas of risk management regarding data usage and vendor compliance.

The IT Data Protection Analyst Associate performs intermediate level work ensuring compliance with document processes, assisting with external audits, and assessing areas of risk management regarding data usage and vendor compliance.

The IT Data Protection Analyst Senior performs full-performance level work overseeing various programs regarding data privacy, data loss prevention, pay card compliance, and manages systems safeguards to ensure data integrety and security.

The IT Data Protection Analyst Specialist performs specialized level work overseeing the citywide records management program which includes developing and implementing policies, procedures, and protocals as it relates to the retention and destruction of protected information.

Essential Duties

Administers the Privacy Program, which includes designing and implementing data privacy protocols and provides guidance to stakeholders on programs subject to data protection regulations, and ensures compliance with federal, state, and local laws.

Conducts privacy and impact assessments, reviewing use agreements, risk determination, develop policies and procedures specific to privacy practices to ensure confidentiality, ensure alignment between areas of technology, and collaborate with agencies and departments to assess needs and develop privacy programs to meet business needs.

Administers the Data Loss Prevention Program, which includes analyzing user behavior and data movement and access to minimize risk to protect information across applications and systems, prevent and mitigate data loss, and implement operational initiatives.

Manages Payment Card Industry compliance citywide, which includes working with finance and external auditor on annual compliance audit.

Manages systems safeguards to ensure adequate safeguards are in place, which includes coordinating efforts with agencies and departments, reviewing vendor business agreements, analyzing end-user behaviors related to data sharing and access, and identifying and classifying sensitive datasets.

Works with stakeholders to include vendors, agencies and departments, and internal information technology personnel to develop policy language, implement internal controls, ensure regulatory compliance, and advise customers on best practices to reduce risk to data integrity and security issues.

Provides guidance to stakeholders regarding privacy laws and regulatory requirements, assists with incident mitigation and breach determination, and notification processes applicable under state and HIPPA requirements.

Collaborates with city attorneys on data use agreements and seek legal guidance on data protection regulations.

Utilizes the data governance protocols to map datasets, which includes data identification and classification.

Develops training materials and presents training to applicable stakeholders based on citywide initiatives.

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

Customer Service – Interacts with customers in a friendly and professional manner, works to resolve issues quickly and effectively, and is knowledgeable about products and services.

Interpersonal Skills – Shows understanding, friendliness, courtesy, tact, empathy, cooperation, concern, and politeness to others and relates well to different people from varied backgrounds and different situations.

Planning and Evaluating – Organizes work, sets priorities, and determines resource requirements; determines short- or long-term goals and strategies to achieve them; coordinates with other organizations or parts of the organization to accomplish goals; monitors progress and evaluates outcomes.

Problem Solving – Identifies problems, determines accuracy and relevance information, and uses sound judgment to generate and evaluate alternatives and to make recommendations.

Reading – Understands and interprets written material, including technical material, rules, regulations, instructions, reports, charts, graphs, or tables; applies what is learned from written material to specific situations.

Working with People - Shows respect for the views and contributions of other team members. Shows empathy, listens, supports, and cares for others, and reconciles conflict

Written Communication - Composes, reviews, edits, and issues written materials for diverse audiences and communicates purpose in a succinct and organized manner that is appropriate for context, time, and place.

Knowledge & Skills

Knowledge US Department of Commerce, National Institute of Standards and Technology (NIST), Cybersecurity and Privacy Frameworks.

Knowledge of Payment Card Industry Data Security Standard (PCI-DSS).

Knowledge of US Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA).

Knowledge of US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security (CJIS) Policy

knowledge of Privacy Framework and Data Protection Frameworks such as NIST, AICPA Privacy Maturity Model, FIPPs and GAPP.

Level of Supervision Exercised

By position, performs lead work or supervises employees within the functional area.

Education Requirement

Bachelor's Degree in Information Technology or a related field based on a specific position(s).

Experience Requirement

Three years of experience with data protection, governance, risk assessment, and compliance with information technology systems.

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

Pressure due to multiple calls and inquiries.
Subject to many interruptions.

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.):

Hearing: Perceiving and comprehending the nature and direction of sounds.
Lifting: Moving objects weighing no more than 10 pounds from one level to another.
Sitting: Remaining in a stationary position.
Talking: Communicating ideas or exchanging information.

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-12
FLSA Code: Y
Established Date: 8/6/2023
Established By: JH
Revised Date:
Revised By:
Class History: This is a new classification.