CARROLLTON
TEXAS

DATE	January 2020
JOB CODE	INFOSECOF
FLSA	EXEMPT
EEO	

JOB TITLE: Information Security Officer
DEPARTMENT/DIVISION: Information Systems
REPORTS TO: Director of Information Systems

SUMMARY: Responsible for establishing the City's enterprise risk and security strategy. Develops directives, policies, and procedures for the organization based on current trends and best practices in the industry. Monitors and tests the enterprise for vulnerabilities and creates plans for enhancement. Creates tactical responses to attacks or security breaches. Creates and manages educational resources and opportunities for City staff regarding information security, including investigation and recovery. Manages staff, vendors, and contractors in the creation of a secure environment through network architecture, trust restrictions, and contractual requirements for outsourced resources. Work requires limited supervision and the use of independent judgment and discretion. Position is also responsible for partnering with the City's Managed Service Provider (MSP), and other city departments in the management of their technology related concerns and resources.

ESSENTIAL JOB FUNCTIONS:

- Develops security related administrative directives, general orders, and standard operating procedures for the enterprise. Monitors industry standards and best practices for regular enhancement of processes and procedures.
- Manages the development of disaster and business recovery protocols to ensure appropriate and timely recovery to security breaches, malicious activity, disasters, or other incidents which impact the City's network or information security. Tests and practices these protocols on a regular basis to ensure business familiarity and reliability of each protocol.
- Manage security framework of the enterprise, including security related applications, appliances, or administrative controls. Assists with the installation, management, upgrade, migration, and enhancement of security products in the City's environment.
- Conducts regular testing for compliance and vulnerability of the City's networks, including penetration testing and PCI compliance testing, among others.
- Maintain compliance with external regulatory controls, such as the Texas Department of Information Resources. Generates and maintains all reporting procedures for compliance related concerns.
- Monitors and responds to security related incidents, including data recovery, business continuity, and mitigation of business impact. Able to respond to such incidents outside of normal business hours in an emergency fashion.
- Responsible for assisting in the training of City staff and contract staff security protocols, risks, and proper habits, including; online learning management, in persons training events, reviewing work accuracy, providing feedback, identifying skill gaps and implementing any necessary skill development or corrective action plans to mitigate gaps.

- Participates in a variety of special projects in support of departmental operations, which may include: analyzing vendor contracts; performing special studies; providing guidance and recommendations to departments to ensure organizational sustainability and maximize organizational efficiency, effectiveness, and performance; recommending cost-conscious decisions and actions; and/or, performing other related activities.
- Performs other duties as assigned, which may involve irregular work hours, including evenings and weekends.

KNOWLEDGE, SKILLS, AND ABILITIES:

- Knowledge of anti-virus applications
- Knowledge of limited or zero-trust environments
- Knowledge of disaster and business recovery practices
- Knowledge of intrusion detection and intrusion prevention applications
- Knowledge of firewall applications
- Knowledge of endpoint security controls
- Knowledge of government operations and processes
- Knowledge of process improvement principles and practices
- Knowledge of data analysis techniques
- Knowledge of research and analysis methods
- Knowledge of strategic planning principles
- Knowledge of data loss prevention techniques
- Knowledge of risk assessment tools, technologies, and methods
- Skilled in designing secure networks, systems, and applications architecture
- Skilled in computer forensics tools and methods
- Skilled in endpoint security solutions
- Skilled in managing projects
- Skilled in developing performance metrics
- Skilled in evaluating quality and reviewing final work products
- Skilled in conducting investigations
- Skilled in analyzing, interpreting, and documenting vendor contracts
- Skilled in analyzing security processes
- Skilled in working with large electronic documents
- Skilled in reading and interpreting technical documents
- Skilled in assessing cost efficiency and effectiveness of municipal operations
- Skilled in conducting benchmark surveys
- Skilled in conducting best practice research
- Skilled in applying independent judgment, personal discretion, and resourcefulness in interpreting and applying guidelines
- Skilled in reading, interpreting, applying, authoring and explaining rules, regulations, policies, and procedures
- Skilled in preparing clear and concise reports
- Skilled in executive level presentations
- Skilled in providing customer service
- Skilled in gathering and analyzing information and making recommendations based on findings and in support of organizational goals
- Skilled in operating a computer and related software applications

- Skilled in communicating effectively with a variety of individuals
- Skilled in security and/or risk management for an on-premise network

MINIMUM QUALIFICATIONS:

- Bachelor’s Degree in Information Systems or a related area of study
- 7 years’ of progressively responsible experience in information technology experience
- 3 years’ of progressively responsible experience in information security
- Must hold, at least one of the following certifications;
    - Certified Information Systems Security Professional (CISSP)
    - GIAC Security Essentials (GSEC)
    - Certified Ethical Hacker (CEH)
    - Certified Information Security Manager (CISM)
    - Certified Protection Professional (CPP)
- Must qualify for and maintain compliance with Criminal Justice Information Systems access requirements

WORKING CONDITIONS:

- Frequent reaching, sitting, talking, seeing, hearing, and manual dexterity
- Occasional climbing, balancing, stooping, kneeling, and crouching
- Occasional lifting and carrying up to 10 pounds
- Work is typically performed in a standard office environment
- Work may be performed in a data-center environment, involving loud noise and temperature irregularity
- Work is occasionally performed in an outdoor environment, with potential exposure to adverse weather conditions

CONDITIONS OF EMPLOYMENT:

- Must pass pre-employment drug test.
- Must pass criminal history check.
- Must pass motor vehicle records check.