Job Specification

Job Title: Chief Information Security Officer	**FLSA Type: E**	**Date Established:10/12/2023**
Department: Dept of Innovation & Technology	**EEO Code: 1.1**	**Date Revised:**
Class Code: 931641	**Reports To: Chief Information Officer**	**Date Approved:10/12/2023**

Job Summary

Partnering with Detroit's leadership team, provides and facilitates vision and leadership for developing, implementing, and supporting security and operational initiatives. The position directs the planning and implementation of enterprise Information Technology security for systems, business operations, and physical technology assets to ensure protection against security breaches. Responsible for auditing existing systems, directing vulnerability mitigation activities, and administering security programs, policies, and standards.

Essential Duties and Responsibilities (*may perform other duties as assigned*)

Essential Functions

- Exercises indirect supervision of staff to assist in security and operations processes.
- Participates in business impact analysis and service prioritization exercises with leadership and Elected officials.
- Participates in the development and maintenance of business continuity and disaster recovery plans.
- Creates proactive processes for event management and daily operations.
- Responsible for advocacy and coordination of Information Technology security.
- Communicates regularly in writing and in person with leadership and end users.
- Secures information, computer, network, processing systems, and new software development.
- Manages the administration of computer security systems and corresponding/associated software including firewalls, intrusion detection systems, cryptography systems, anti-virus software, and event log management.
- Recommends and implements changes in security policies and practices in accordance with changes in applicable law.
- Provides resolution to security problems.
- Assesses and communicates security risks associated with purchases or practices performed by the City.
- Collaborates to establish and maintain a system for ensuring that security and privacy policies are met.
- Promotes and oversees strategic security relationships between internal resources and external entities, including government, vendors, and partner organizations.
- Remains aware of trends and issues in the security industry, including current and emerging technologies; advises, counsels, and educates leadership on issues and trends, importance, and financial impact.
- Participates as a contributor to city leadership and elected officials concerning the City's Information Technology security strategies.

- Leads strategic security plans; achieves business goals; prioritizes defense initiatives and coordinates the evaluation, deployment, and management of current and future security technologies; utilizes a risk-based assessment methodology.
- Develops and communicates security strategies and plans to leadership and elected officials, staff, partners, customers, and stakeholders.
- Develops, implements, maintains, and oversees enforcement of policies, procedures, and associated plans for system security administration and user system access.
- Ensures dissemination of security information throughout the organization and clarity of roles and responsibilities.
- Informs, mentors, and coaches senior management, staff, and teams in potential and emerging cyber security threats, vulnerabilities, and control techniques.
- Designs and delivers cyber-security awareness training.
- Defines and communicates plans, procedures, policies, and standards for the organization for acquiring, implementing, and operating new security systems, equipment, software, and other technologies.

Nonessential Functions

- If a local declaration of emergency or disaster is declared by the city of Detroit, employee may be required to work as a Disaster Service Worker.
- Performs other duties as appropriate or necessary for performance of the job.

Qualifications (required):

- Bachelor's degree or equivalent from an accredited college or university with major coursework in business, Information Systems, Public Administration, or a related field required.
- Five (5) years of experience in managing Information Technology and/or security operations required.

Equivalent combinations of education and experience may be substituted to meet the education and experience requirements of this position.

Qualifications (preferred):

- Master’s degree from an accredited college or university specializing in Cyber Security.
- Certification in Cyber Security best practice (CISSP, Security +, CISA, CISM, etc.)
- Experience managing cross functional teams with a proven record of success.
- Ten (10) years of experience in managing Cyber Security operations required.

Knowledge, Skills, and Abilities

- General office practices and procedures.
- Routine software and business applications including, but not limited to, word processing, spreadsheets, presentation software, and databases.
- Communicate clearly and concisely, both verbally and in writing.
- Adhere to city rules, regulations, policies, and standard operating procedures.
- Establish and maintain effective working relationships with other City employees, representatives of other agencies and organizations, and members of the community.
- Regular, predictable attendance.
- Understand computer systems and network characteristics, features, and integration capabilities.
- Apply Information Technology in solving security problems.
- Application of applicable laws and regulations as they relate to security, including HIPAA and CJIS requirements.
- Leadership methods and management skills.

- Set and manage priorities
- Strategies and application of negotiating.
- Ability to present ideas in business-friendly and user-friendly language.
- Perform duties independently without close supervision
- Attention to detail.
- Analytical, evaluative, and problem-solving abilities.
- Practices and application of customer service.
- Ability to motivate in a team-oriented, collaborative environment.

Licenses, Certifications, and Other Special Requirements:

- Certified Information Systems Security Professional (CISSP) according to the International Information Systems Security Certification Consortium is strongly preferred.

Physical Demands

- Strength – Sedentary
- Movement – Occasionally
  Stooping, reaching, handling, and finger dexterity.
- Auditory – Not Limited
  Talking and hearing.
- Vision – Required
  Near and far acuity

Work Environment

- Equipment
  Office Equipment
- Computer use – Constantly

The above statements reflect the general nature and level of work performed by employees assigned to this class. Incumbents may be required to perform job-related responsibilities and tasks other than those stated in this specification. Essential duties may vary from position to position.

Notes: