CLASS TITLE | INFORMATION SECURITY MANAGER

PAY GRADE: EX-44| www.cityoftulsa.org/pay

Class Code: 1141 **Effective Date : 12/21/2022**

*****THIS CLASSIFICATION INCLUDES PAY INCREASE OPPORTUNITIES - OUTLINED BELOW*****

PURPOSE OF THE CLASSIFICATION: Under general supervision is responsible for coordinating information security implementations, monitoring and maintaining network and computer security policies with a focus on identifying and mitigating IT vulnerabilities, and designing and planning solutions to continuously improve information security in order to support compliance utilizing best practices.

ESSENTIAL TASKS:

- Plans, coordinates, and controls security services operations and projects related to information security
- Supervises, conducts, and coordinates the performance of network/computer security testing, forensics, penetration and security compliance, auditing, and assisting or coordinating implementation of security solutions and tracking resolution of findings and preparing reports
- Advises senior management of changes in the technical, legal, and regulatory arenas impacting information security and computer crime
- Serves as an expert technical resource in advising and assisting all departments in information security issues both proactively and reactively
- Establishes, leads, and participates in Information Security teams comprised of key individuals from the Information Technology (IT) department and other City departments designed to identify key security strategies to meet business needs, comply with regulatory requirements and best practices, and leverage available technology
- Develops, implements, evaluates, and maintains an information security awareness and training program with IT and City training staffs
- Implements and administers the information security training program and associated staff
- Oversees and administers a comprehensive enterprise-level information security policy program including the creation, implementation, review, and documentation of enterprise-level information security policies and procedures
- Acts as a liaison with the Public Safety Security staff regarding overlapping information security issues, including investigations and badge access, as well as other external organizations, cybersecurity industry partners, and government agencies.
- Must report to work on a regular and timely basis

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential tasks.

QUALIFICATIONS:

Training and Experience: Must meet the following option or an equivalent combination of training and experience per Personnel Policies and Procedures, Section 100:

1. (a) Completion of 120 hours from an accredited college or university including coursework in fields relevant to the essential tasks listed in this job description; **and,**
   (b) Four (4) years' experience relevant to the essential tasks listed in this job description; **or,**
   (c) Five (5) years' experience in legal and/or finance with Security+ certification

PAY INCREASE OPPORTUNITY

Employee will be eligible for a one step increase upon completion of thirty (30) accredited college hours and one (1) year employment in the position.

Employees requesting proficiency or progression increase must not be on a City Performance Improvement Plan at the time of the request.

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the Comptia Security+ certification if not already possessed and nine (9) months of employment in the position. *The Security+ certification is mandatory within twelve (12) months of employment in the position without prior security experience or at first opportunity based upon the availability of training.*

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the Comptia Network+ certification and nine (9) months of employment in the position. *The Network+ certification is mandatory within twelve (12) months of employment in the position or at first opportunity based upon the availability of training.*

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the ISC^2 Certified Authorization Professional (CAP) certification and twelve (12) months of employment in the position.
  The CAP certification is mandatory within thirty (30) months of employment in the position or at first opportunity based upon the availability of training.

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the ISC^2 Certified Information Systems Security Professional (CISSP) certification "Associate of ISC^2" level and eighteen (18) months of employment in the position.
  The ISC^2 Certified Information Systems Security Professional (CISSP) certification "Associate of ISC^2" level is required within 18 months of employment in the position or at first opportunity based upon the availability of training.

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the IACIS Certified Forensic Computer Examiner certification and two (2) years of employment in the position.

- Employee will be eligible for the equivalent of a five (5) percent increase upon attaining the CISSP certification "Associate of ISC^2" level or higher of the same certification and five (5) years of employment in the position.

- Employee will be eligible for the equivalent of a one (1) step increase upon completion of the ISACA Certified Information Security Manager (CISM) certification; **or,** the CISSP Information Systems Security Management Professional (CISSP-ISSMP); concentration; and five (5) years of employment in the position.
  The ISACA Certified Information Security Manager (CISM) certification or the CISSP Information Systems Security Management Professional (CISSP-ISSMP) is required within 5 years of employment in the position or at first opportunity based upon the availability of training.

- Employee will be eligible for the equivalent of a three percent (3%) increase upon attaining the ISACA Certified Information Systems Auditor (CISA) certification and five (5) years of employment in the position.
  The ISACA Certified Information Systems Auditor (CISA) certification is required within 5 years of employment in the position or at first opportunity based upon the availability of training.

Knowledge, Abilities and Skills:

Knowledge of:

- Considerable working knowledge of information technology, networking, transmission protocols, computer systems, databases, and the security methods and tools related to each, including, but not limited to, encryption, intrusion detection, network design, and networking and security hardware
- Knowledge of case law to accurately determine potential liability and information security requirements
- Knowledge and ability to interpret legal statutes and regulations; some knowledge of cost-benefit analysis, finance, or economics.

Ability to:

- Ability to analyze security systems from both technically and financially feasible aspects
- Ability to determine long-term information security operational needs
- Ability to keep abreast of technological advancements to include maintaining membership in governmental and information security programs and information security certifications
- Ability to effectively manage subordinates engaged in various information security activities
- Ability act as a project manager for multiple, concurrent, enterprise-level projects simultaneously
- Ability to communicate effectively both verbally and in writing
- Ability to successfully negotiate highly sensitive issues
- Ability to conduct meetings with a good knowledge of formal rules of order
- Ability to utilize the highest level of interpersonal skill in order to understand, select, develop and motivate people at any level within or outside the organization
- Ability to develop enterprise-level training policies and programs, disseminate and manage requirements and notifications, coordinate training administration, and ensure enterprise training accountability
- Ability to act as the subject matter expert and primary liaison for enterprise-level policy creation to all departments, ensuring adherence to proper creation procedure, proper notice, consideration, redress, and implementation.

Physical Requirements: Physical requirements include arm and hand steadiness and finger dexterity enough to use a keyboard and telephone; occasional lifting and carrying up to 20 pounds; occasional pushing and pulling up to 10 pounds; may be subject to walking, standing, sitting, reaching, balancing, bending, kneeling, handling, smelling and twisting; and vision, speech and hearing sufficient to perform the essential tasks.

Licenses and Certificates:

1. Possession of a valid Oklahoma Class “D” Driver License; and
2. Possession of the Comptia Security+ certification within twelve months from date of employment; **and,**
3. Possession of the Comptia Network+ certification within twelve months from date of employment; **and,**
4. Possession of the ISC^2 Certified Authorization Professional (CAP) certification within thirty months from date of employment; **and,**
5. Possession of ISC^2 Certified Information Systems Security Professional (CISSP) certification “Associate of ISC^2” level upon 18 months from date of employment; **and,**
6. Possession of the Certified Forensic Computer Examiner (CFCE) upon two (2) years of employment **and,**
7. **P**ossession of ISC^2 Certified Information Systems Security Professional (CISSP) certification upon five (5) years of employment; **and,**
8. Possession of the ISACA Certified Information Security Manager (CISM) certification or CISSP Information Systems Security Management Professional (CISSP-ISSMP) concentration certification upon five (5) years of employment; **and,**

9. Possession of the Certified Information Systems Auditor (CISA) certification upon five (5) years of employment

WORKING ENVIRONMENT: Working environment is primarily indoors in an office environment.

EEO Code: E-01
Group: Engineering, Planning, and Technical
Series: Communications Operations and Maintenance