CLASS TITLE: INFORMATION SECURITY MANAGER

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 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 and leads an Information Security team 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 and best practices and leverage available technology
• Develops, implements, evaluates, and maintains an information security awareness and training program
• 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

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

QUALIFICATIONS:
Training and Experience:
Graduation from an accredited college or university with a bachelor's degree in computer science, management information systems, or other related field, and five (5) years of experience in information security, legal and/or finance; or an equivalent combination of training and experience per Personnel Policies and Procedures, Section 128.

Employee will be eligible for a two percent (2%) increase upon completion of the ISC² Certified Authorization Professional (CAP) certification and nine (9) months of employment in the position. Employee will be eligible for a two percent (2%) increase upon completion of the GIAC Security Leadership (GSLC) certification and nine (9) months of employment in the position. Employee will be eligible for a two (2%) increase upon completion of the CompTIA Security+ and (1) one year of employment in the position. Employee will be eligible for a two (2%) increase upon completion of the GIAC Information Security Fundamentals (GISF) certification and one (1) year of employment in the position. Employee will be eligible for a three percent (3%) increase upon completion of the ISC² Certified Information Systems Security Professional (CISSP) certification “Associate of ISC²” level and eighteen (18) months of employment in the position. Employee will be eligible for a five percent (5%) increase upon completion of the ISC² Certified Information Systems Security Professional (CISSP) certification and five (5) years of employment in the position (see licenses and certifications section below).

Knowledge, Abilities and Skills:
Considerable working knowledge of information technology, networking, transmission protocols, computer systems, databases, and the security methods and tools related to each, to include 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 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; and 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 Certification:** Possession of valid Oklahoma Class “D” Operator’s license. Possession of the ISC² Certified Authorization Professional (CAP) certification within nine months from date of employment; possession of the GIAC Security Leadership (GSLC) certification within nine months from date of employment; possession of the CompTIA Security+ within one year from date of employment; possession of the GIAC Information Security Fundamentals (GISF) certification within one year from date of employment; possession of ISC² Certified Information Systems Security Professional (CISSP) certification “Associate of ISC²” level within 18 months from date of employment; and possession of ISC² Certified Information Systems Security Professional (CISSP) certification upon five (5) years of employment.

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

Class Code: 1141  
EEO Code: E-01  
Pay Code: EX-44  
Group: Engineering, Planning, and Technical  
Series: Communications Operations and Maintenance  
Effective date: January 25, 2015