

INFORMATION SECURITY MANAGER

Summary:

The position of Information Security Manager is a high-level security positions which reports to and performs tasks under the direction of the Chief Information Security Officer (CISO). This is a hands-on management position which requires advanced technical skills, as well as management abilities. The Information Security manager will coordinate the efforts of the Information Security Group, including all staff, technology, projects, and incident response. In addition, this position will provide support across the city, including information technology, personnel, communications, law, and other departments and will identify security initiatives and standards. Direct reports may include technical and support personnel such as Security Analysts, Security Business Analysts, Security Engineers, and Security Administrators.

Responsibilities:

- Oversee a team of security personnel who safeguard the City's assets, intellectual property, information systems and the physical security of Information Technology processing facilities.
- Coordinate hiring, training, and evaluation of security personnel and the development of education/training programs to ensure appropriate awareness of security policies, procedures, and standards.
- Identify protection goals, objectives and metrics consistent with the City's strategic plan.
- Manage the development and implementation of City-wide security policies, standards, guidelines and procedures to ensure ongoing maintenance of security.
- Maintain relationships with other localities, state and federal law enforcement and other related government agencies.
- Physical security responsibilities will include asset protection, access control systems to information processing facilities, video surveillance and more.
- Information protection responsibilities will include network security architecture, network access and monitoring policies, employee education and awareness and more.
- Oversee Incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.

Required Skills:

- Must have strong technical knowledge of networking, data structures, directory systems, internet, security, and other technologies.
- Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the management team and who is able to communicate security related concepts to a broad range of technical and non-technical staff.
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor management.
- Must have strong working knowledge of pertinent law and the law enforcement community.
- Must have a solid understanding of information technology and information security.

Education required:

BS in related field or 5 years relevant work experience in field
Professional information security certification preferred - such as CISSP, CISM, etc.
Working knowledge with industry standards such as NIST, SANS, COBIT, and ISO

Experience Required:

10+ years in Information Technology field
5+ years in Information Security
Worked and/or consulted in Federal, State, City or local government *desirable*