IT SECURITY ADMINISTRATOR

SUMMARY: Under general direction form the IT Director, will work collaboratively with all IT Divisions and other City Departments and will design and implement IT security solutions and or services to ensure integrity of the City's intellectual property including data and infrastructure. Recommends and provides oversight of the necessary controls and procedures to establish and preserve the City's entire Information Technology security posture. He\she will proactively monitor all IT infrastructure internal and perimeter network controls, provide preemptive action for alerts or perceived vulnerabilities, and provide reports regarding effectiveness against threats, breaches and compliance with all regulatory requirements.

ESSENTIAL FUNCTIONS: *(Essential functions, as defined under the Americans with Disabilities Act, may include the following tasks, knowledge skills, and other characteristics. This list is ILLUSTRATIVE ONLY, and is not a comprehensive listing of all functions and tasks performed by incumbents of this class.)*

DUTIES AND RESPONSIBILITIES: (Which are **not** in any hierarchical order)

1. Design, implement and maintain all IT related security systems to protect City assets and information using industry best practices and while maintaining compliance with applicable federal, state, and City Policies.
2. Ensure that all system and data access controls are implemented, maintained and monitored through a security methodology that supports daily operations and aligns with security compliance requirements.
3. Develop, implement and maintain Information Security Policies and Procedures to include system hardening, password management, data handling and management (at rest and in transit), and incident management and reporting.
4. Work collaboratively with IT Divisions and vendors to design, implement and proactively maintain IT Security solutions and systems. Develop and maintain documentation and diagrams for same.
5. Conduct and proactively manage periodic vulnerability assessments, audits of internal operating procedures, and develop reports and remediation plans accordingly.
6. Serve as primary point of contact for all other IT related audits and develop reports and remediation plans accordingly.
7. Develop, implement and maintain internal investigation procedures as it relates to IT security including access control, content filtering, appropriate handling of IT intellectual property, and appropriate use of IT assets.
8. Develop, implement and maintain an incident management solution to include proactive response, escalation, and remediation procedures; ongoing and in the event of an organizational or wide-spread security breach.
9. Develop, implement and maintain an organizational IT Security Awareness program to include training and marketing.
10. Research and understand and prepare for emerging security threats, vulnerabilities and effective countermeasures.
11. Working collaboratively with IT Divisions and Departments, develop a long term strategy for IT Security as part of the IT Strategic Plan.

KNOWLEDGE, SKILLS AND ABILITIES:

- Advanced knowledge and experience with Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), Data Loss Prevention solutions (DLP), Content Filtering solutions, two factor authentication, single sign on (SSO), and Firewalls.
- Advanced knowledge and experience with Cisco network and security platforms including: routers and switches, ASA, Ironport web and email filtering solutions.
- Expert level understanding of network routing and switching architecture, design and troubleshooting.
- Expert level understanding of packet sniffer software and tools.
- Current experience with Microsoft Windows and corporate networking design including LDAP, AD, DNS, etc.

IT SECURITY ADMINISTRATOR

- Experience with traditional IT Infrastructure platforms and connectivity including LAN\WAN\VLAN's, IP, FTP and SFTP protocols, servers, storage, telephony, site to site tunneling, etc.
- Ability to establish and maintain effective working relationships with those contacted in the course of work.

PHYSICAL REQUIREMENTS AND WORK ENVIRONMENT: Work involves sedentary to light work in an office setting. There is occasional need to sit, talk, or hear, stand, walk, reach with hands and arms and lift light items (up to 25 pounds). There is frequent need to talk or hear, use hands to finger, handle or feel. There is occasional need to perform work outdoors with exposure to weather conditions when performing on-site inspections of projects and perform other similar actions during the course of the workday. The City of West Palm Beach promotes and maintains a drug/alcohol free work environment through the use of mandatory pre-employment and random drug testing for certain employees.

MINIMUM QUALIFICATION: Bachelor of Science degree from an accredited college or university with a major in an Information Technology discipline, or related field and eight (8) years of progressively responsible experience in an IT Security Administrator role, or any equivalent combination of experience. Current Certified Information Security Systems Professional (CISSP) or ability to obtain within six months of hire.

A valid driver's license from any state (equivalent to a State of Florida Class E) may be utilized upon application; with the ability to obtain the State of Florida driver's license within 30 days from day of appointment