INFORMATION TECHNOLOGY MANAGER
FLSA: EXEMPT

Grade 34: $84,693 - $135,509

GENERAL DEFINITION

Position assists in all aspects of administration, direction, and management of the City's Information Technology Services functions. Responsible for the day-to-day operations of the in-place security solutions while and the detection, analysis, containment, eradication, and recovery from security breaches detected by those systems. Secondary tasks may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines, and procedures as well as conducting vulnerability audits and assessments. This position entails great responsibility and proper time management because the job requests constant monitoring many departmental day to day operations. Acts as a point of contact between the staff and Assistant Director of ITS, and may be called to act in that capacity in the absence of the Assistant Director of ITS.

This skilled technical position is responsible for administering and maintaining security controls focused on network security across the City's enterprise in accordance with existing policies, procedures, and security best practices. This skilled position will be responsible for safeguarding privileged information and prevention of unauthorized access to City-wide resources.

- The IT Security Administrator performs core functions for the enterprise as follows: is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures, and guidelines.
- is responsible for articulating technical security requirements, monitoring the effectiveness of the IT security controls framework, and assisting in raising security awareness and policy compliance among workforce members.
- Acts in the role of Assistant Director of ITS, when necessary.

ESSENTIAL JOB DUTIES

The list of duties and functions, as outlined herein, is intended to be representative of the type of tasks performed within this classification. They are not listed in any order of importance. The omission of an essential function does not preclude management from assigning duties not listed herein if such functions are a logical assignment to the position.

INFORMATION TECHNOLOGY MANAGER
FLSA: EXEMPT

Grade 34: $84,693 - $135,509

STRATEGY & PLANNING

- Participate in the planning and design of enterprise security architecture where appropriate.
- Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures) where appropriate.
- Participate in the planning and design of an enterprise Incident Response Plan, Business Continuity Plan and Disaster Recovery Plan where appropriate.
- Promotes security awareness and Cybersecurity goals with all City staff.

ACQUISITION & DEPLOYMENT

- Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Review current security measures, recommend, and implement additional security solutions or enhancements.
- Perform the deployment, integration, and initial configuration of all new security solutions and of any enhancements to existing security.

OPERATIONAL MANAGEMENT

- Provides day-to-day support of the information security program.
- Ensures that IT Security best practices and configurations are included in network, desktop, server, and mobile configurations are adhered to.
- Design, document, and maintain security controls.
- Works with other departments to define role-based access control, segregation of duties, and helps to implement secure business processes.
- Monitor security threats, analyze vulnerability assessments, and balance security with the operational mission of the City.
- Monitor all in-place security solutions for efficient and appropriate operations.
- Conduct research, evaluates, pilot deployments of security products/features and

provide recommendations for improvements of existing security controls.

- Respond to security related issues and other requests from various departments, and works collaboratively across multiple teams, to communicate and manage expectations during the resolution of a detected incident.
- Assures the Confidentiality, Integrity, and Availability (CIA) of information stored on City computers or networks by ensuring inadvertent modification and/or the non-disclosure of the City's information to unwanted parties.
- Assist in assessing technological risks.
- Collaborate with project stakeholders to make recommendations that help achieve City business and functional goals while meeting security requirements.

EXAMPLES OF DUTIES

- Next-Gen Firewall and security appliances log collection and correlation using available tools
- Support, maintain, and monitor Next-Gen antivirus protection operations by maintaining malware protection through updates and ensuring controls are effective.
- Ensure that IT security best practices and configurations are included in network, desktop, server, wireless, VoIP, and mobile configurations.
- Administers and maintains end user accounts, permissions, and access rights.
- Audit user access and activities from actively administered log files.
- Identify and defend systems and data against unauthorized access, modification and/or destruction.
- Ensure continuous monitoring of data, systems, and network security.
- Monitor network traffic for suspicious activity.
- Train fellow employees in security awareness and procedures.
- Promptly respond to all security incidents and provide thorough post-event analyses and remediations.

KNOWLEDGE, SKILLS & ABILITIES

- Extensive experience with and knowledge of the Sentinel One security suite including EPP, EDR and Ranger.

- Experience with Palo Alto firewalls and associated management tools.
- Familiarity with KnowBe4 for Security, Education, Training, and Awareness (SETA).
- Strong understanding of AD, IP, TCP/IP, and other network administration protocols.
- Experience with the following access control schemes:
    - Role-based Access Control (RBAC)
    - Mandatory Access Control (MAC)
    - Discretionary Access Control (DAC)
- Strong understanding of Windows Server 2012, 2016, & 2019, and Windows 10 or higher.
- Knowledge and experience in using automated tools for Windows OS software updates and other software vendor software updates, hot fixes, and patches, etc.
- Possess a high degree of integrity and trust along with the ability to work independently on complex technical issues.
- Proven analytical and problem-solving abilities with keen attention to detail.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Good written, oral, and interpersonal communication skills.
- Ability to conduct research into IT security issues and products as required.
- Ability to present ideas in business-friendly and user-friendly language.
- Highly self-motivated and directed.
- Team-oriented and skilled in working within a collaborative environment

PHYSICAL REQUIREMENTS

The City of Oakland Park is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act (42 U.S. C. 12101 et. seq.), the City of Oakland Park will provide reasonable accommodations to qualified individuals with disabilities and encourages both prospective and current employees to discuss potential accommodations with the employer. The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job.

- The ability to stand, sit, walk, talk, and hear.
- Must be able to operate objects, tools or controls and reach with arms and hands.
- Walk up or down stairwells, ladders, or steps.

INFORMATION TECHNOLOGY MANAGER
FLSA: EXEMPT

Grade 34: $84,693 - $135,509

- The employee must frequently lift and/or move up to 35 pounds.
- Vision ability includes close and peripheral vision, and depth perception.

Oral communications abilit**MINIMUM ACCEPTABLE EDUCATION, TRAINING & EXPERIENCE**

- Associate's degree from an accredited two (2)year college or university with major course work in computer science or related field, or equivalent work experience. A bachelor's degree is preferred.
- A minimum of two (2) to four (4) years of relevant experience in IT Security, Audit, or Compliance inclusive of implementing security measures and deploying, configuring, maintaining, and integrating security solutions.
- Maintain one or more of the following certifications in good standing, or be able to obtain this within nine (9) months of employment:
    - CompTia Security+
    - CISM - Certified Information Security Manager (CISM)
    - CISSP - Certified Information Systems Security Professional (CISSP)
    - CEH - Certified Ethical Hacker (CEH)
    - OSCP - Offensive Security Certified Professional (OSCP)
    - CCSP - Certified Cloud Security Professional (CCSP)
    - MTA/SF - Microsoft Technology Associate (MTA) Security Fundamentals
    - CSX Cybersecurity Fundamentals Certificate
    - CCNA – Security

I _____ have read and acknowledge receipt of the job classification.

_____ _____

Employee signature Date