

**City of Dunedin, Florida**  
Class Description

**JOB TITLE: IT Network Security Analyst**  
Information Technology Services Department

**GENERAL STATEMENT OF JOB**

Under general direction, ensures the secure operation of the City's in-house computer systems, servers, and network connections against intrusion and anomalies. Employees in this classification are responsible for monitoring network traffic for security incidents and events, investigating incidents and respond to events in real time, write detailed incident response reports, install and operate firewalls, encryption programs, and other security software, fix vulnerabilities, develop and promote best practices for information security. conduct threat research and perform periodic risk assessments and penetration tests. Work is performed with limited direction and considerable latitude for the use of initiative and independent judgment. This position reports to the Director of Information Technology Services.

**SPECIFIC DUTIES AND RESPONSIBILITIES**

**ESSENTIAL JOB FUNCTIONS**

***The duties recorded below are representative of the duties of the class and are not intended to cover all the duties performed by incumbent(s) of any particular position.***

Develops, oversees, and maintains policies, procedures and associated plans for system security administration and user system access based on industry-standard best practices.

Coordinates and oversees the end-user cyber security awareness training and compliance program.

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Assesses the need for any security reconfigurations (minor or significant); makes recommendations and executes them if approved.

Conducts research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.

Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy.

Coordinates all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, and anti-virus software; manages and ensures the security of databases and data transferred both internally and externally.

Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment.

Oversees penetration testing of all systems to identify system vulnerabilities.

Collects, processes, analyzes, and disseminates cyber threat/warning assessments.

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities.

Keeps current with emerging security alerts and issues; downloads and tests new security software and/or technologies.

Consults with the Department Director and users to conduct information assessments to determine user needs and to define systems requirements including the reviewing, maintaining and documenting of systems minimum standard requirements.

### **ADDITIONAL JOB FUNCTIONS**

***While the following tasks are necessary for the work of the unit, they are not an essential part of the purpose of this position and may also be performed by other unit members.***

Installs, configures, manages and maintains mission critical enterprise security infrastructure and their corresponding or associated software including firewalls, routers, switches, intrusion detection systems, VPN and anti-virus software.

Recommends, schedules (where appropriate), and applies fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.

Drives investigation of security breaches including coordinating with internal and external entities on communications, documentation, and resolution of issue.

Participate on cross-functional project teams to ensure technology security guidelines are followed.

Develops security configuration for network and wireless LANs, PC's, servers, laptops, mobile and handheld devices.

Coordinates security requirements for application development.

Monitors server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity; interprets activity and makes recommendations for resolution.

Performs security audits of the network infrastructure.

Oversees and/or performs penetration testing of all systems to identify system vulnerabilities.

Initiates, facilitates, and promotes activities to create information security awareness for computer users.

Performs related duties as required.

### **MINIMUM TRAINING AND EXPERIENCE**

Requires a Bachelor's degree in Computer Science, Cybersecurity and Information Assurance, or other relevant field, supplemented by a minimum of five years of experience in computer systems configurations, analysis, or engineering. Experience working with data and wireless communications, as well as email and voice messaging systems is a must.

An equivalent combination of education, training and experience that provides the required knowledge, skills and abilities may be considered in lieu of the experience.

### **SPECIAL REQUIREMENTS**

Broad hands-on knowledge of firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices.

Knowledge of applicable practices and laws relating to data privacy and protection.

In-depth technical knowledge of network, PC, and platform operating systems.

Working technical knowledge of current systems software, protocols, and standards.

Strong knowledge of TCP/IP and network administration/protocols.

Ability to self-motivate.

Ability to travel to various City facilities to support network equipment.

Must possess a valid Florida driver's license.

This is a Category A position for the purposes of Emergency Management. Employees in this category may be assigned to work a variety of schedules, including compulsory work periods in special, emergency, and/or disaster situations. Category A employees are required to stay on premises during a declared state of emergency, or as otherwise mandated.

### **PERFORMANCE INDICATORS**

**Knowledge of Job:** Has thorough knowledge of the methods, procedures and policies as they pertain to the performance of essential duties of the IT Network Security Analyst. Is knowledgeable in the laws, ordinances, standards and regulations pertaining to the specific duties and responsibilities of the position. Is able to make sound, educated decisions. Clearly understands any occupational hazards and adheres to all safety precautions inherent in performing the essential functions of the work. Has the ability to speak, write and understand the English language.

### **PERFORMANCE APTITUDES**

**Data Utilization:** Requires the ability to evaluate, audit, deduce, and/or assess data and/or information using established criteria. Includes exercising discretion in determining actual or probable consequences, and in referencing such evaluation to identify and select alternatives. Is able to assemble and analyze information and make written reports and records in a concise, clear and effective manner.

**Human Interaction:** Requires the ability to provide guidance, assistance, instruction and/or interpretation to others on how to apply procedures and standards to specific situations. Shares knowledge with managers, supervisors and co-workers for mutual benefit. Develops and maintains cooperative and courteous relationships inter- and intra-departmentally, and with external entities with whom the position interacts. Tactfully and effectively handles requests, suggestions and complaints in order to establish and maintain good will. Knows how to maintain effective relationships with personnel of other departments, professionals and members of the public through contact and cooperation. Is able to provide effective user training and support as required.

**Equipment, Machinery, Tools and Materials Utilization:** Requires the ability to set up small to moderate scale equipment and machinery. Includes the ability to install and alter various components of such according to work orders and/or specifications. Has knowledge of the areas of computer software/hardware installation and maintenance,

system design and installation, government procurement, user training and support, etc. Has knowledge of and skill in the use of modern office equipment.

**Verbal Aptitude:** Requires the ability to use a wide variety of reference, descriptive, advisory and/or design data and information. Has thorough knowledge of terminology and related professional languages used within the department as such pertain to work responsibilities. Has knowledge of proper English usage, grammar, vocabulary and spelling. Requires the ability to speak, write and understand the English language.

**Mathematical Aptitude:** Requires the ability to perform moderately complex algebraic and geometric operations; ability to utilize principles of basic probability and statistical inference. Has the mathematical ability to handle required calculations.

**Functional Reasoning:** Requires the ability to apply principles of logical or synthesis functions. Ability to deal with several concrete and abstract variables, and to exercise independent judgment to apply facts and principles for developing approaches and techniques to problem resolution.

**Situational Reasoning:** Requires the ability to exercise the judgment, decisiveness and creativity required in situations involving evaluation of information against measurable or verifiable criteria. Has the ability to plan and develop daily, short- and long-term goals related to organizational purposes. Is able to take the initiative to complete the duties of the position without the need of direct supervision. Has the ability to plan, organize and prioritize daily assignments and work activities. Is able to read and interpret complex materials pertaining to the responsibilities of the job.

### **ADA COMPLIANCE**

**Physical Ability:** The essential functions of the job require: sitting approximately four (4) to six (6) hours per day, standing approximately two (2) to (4) hours per day, and walking approximately one (1) to two (2) hours per day. Frequently the job requires: bending/stooping, crawling, fine manipulations, grasping, kneeling, pushing, reaching, repetitive motion, and light lifting/carrying (objects weighing less than 15 pounds). Occasionally the job requires: climbing and pulling, and moderate lifting/carrying (objects weighing 15 to 44 pounds). Rarely the position requires: heavy lifting/carrying (objects weighing 45 pounds and over).

**Sensory Requirements:** Some tasks require visual and auditory perception and discrimination as well as oral communications ability.

**Environmental Factors:** Tasks are regularly performed without exposure to adverse environmental conditions. Tasks may require extensive VDT exposure.

***The City of Dunedin is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the employer will provide reasonable***

***accommodations to qualified individuals with disabilities and encourages both prospective and current employees to discuss potential accommodations with the employer.***

Approved:



August 1, 2024

---

Michael Nagy  
Director, Information Technology Services

---

Date