Code: 06A7
Family: Information Technology
Service: Administrative
Group: Clerical, Accounting, and General Office
Series: Information Technology

CLASS TITLE: IT SECURITY ANALYST-INSPECTOR GENERAL

CHARACTERISTICS OF THE CLASS

Under general supervision, the class works as a specialist in the administration of information technology security solutions and tools for the Office of Inspector General (OIG), and performs related duties as required

ESSENTIAL DUTIES

- Configures and administers the department's security technologies relevant to security operations for all on-premises, hosted, cloud infrastructure, storage, applications systems and networks
- Performs continuous monitoring of the department's security solutions and system logs for threat indicators
- Analyzes and correlates incident event data to develop and document preliminary root cause and corresponding remediation strategy
- Works closely with team members, other business units, and vendors to ensure new systems, applications, subscriptions, services, and processes meet security and vulnerability management requirements
- Executes and proposes improvements to procedures related to security practices and processes to protect department's networks
- Ensures users, service delivery, and systems adhere to documented information technology security standards and protocols
- Monitors the application security community for public-facing security issues, as well as to learn new tactics that can be used in testing
- Assists in the implementation and documentation of compliance with cybersecurity frameworks (e.g., NIST, COBIT, and CIS Controls)
- Assists in developing material for conducting security awareness training and phishing simulations, as required

***NOTE**: The list of essential duties is not intended to be inclusive; there may be other duties that are essential to particular positions within the class.*

MINIMUM QUALIFICATIONS

Education, Training, and Experience

- Graduation from an accredited college or university with a Bachelor's degree in Computer Science, Information Technology/Systems, or a directly related field plus two years of professional work experience in information security, or an equivalent combination of education, training and experience, provided that the minimum degree requirement is met.

Licensure, Certification, or Other Qualifications

- None

WORKING CONDITIONS

- General office environment

EQUIPMENT

- Standard office equipment (e.g., telephone, printer, photocopier, fax machine, calculator)
- Computers and peripheral equipment (e.g., personal computer, computer terminals, hand-held computer, scanner)

PHYSICAL REQUIREMENTS

- No specific requirements

KNOWLEDGE, SKILLS, ABILITIES, AND OTHER WORK REQUIREMENTS

Knowledge

Moderate knowledge of:

- *information security concepts, toolsets and solutions
- *network infrastructure devices (e.g., firewalls, routers and switches)
- *Security Incident and Event Management (SIEM) solutions
- *security solutions (e.g., antivirus, encryption, endpoint detection and response, data loss prevention, intrusion detection and prevention, systems patching, vulnerability management, and threat intelligence)
- *new and emerging IT security technologies/trends
- *applicable computer software packages and applications

Knowledge of applicable City and department policies, procedures, rules, and regulations

Skills

- *ACTIVE LISTENING – Give full attention to what other people are saying, take time to understand the points being made, ask questions as appropriate, and not interrupt at inappropriate times
- *CRITICAL THINKING – Use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions, or approaches to problems
- *LEARNING STRATEGIES – Select and use training/instructional methods and procedures appropriate for the situation when learning or teaching new things
- COMPLEX PROBLEM SOLVING – Identify complex problems and review related information to develop and evaluate operations and implement solutions
- *JUDGEMENT AND DECISION MAKING – Consider the relative costs and benefits of potential actions and choose the most appropriate one

Abilities

- COMPREHEND ORAL INFORMATION – Listen to and understand information and ideas presented through spoken words and sentences
- COMPREHEND WRITTEN INFORMATION – Read and understand information and ideas presented through spoken words and sentences
- SPEAK – Communicate information and ideas in speaking so others will understand
- WRITE – Communicate information and ideas in writing so others will understand
- REASON TO SOLVE PROBLEMS – Apply general rules to specific problems to produce answers that make sense

- MAKE SENSE OF INFORMATION – Quickly make sense of, combine, and organize information into meaningful patterns

Other Work Requirements

- INITIATIVE – Demonstrate willingness to take on job challenges
- ADAPTABILITY / FLEXIBILITY – Be open to change (positive or negative) and to considerable variety in the workplace
- DEPENDABILITY – Demonstrate reliability, responsibility, and dependability and fulfill obligations
- INDEPENDENCE – Develop own ways of doing things, guide oneself with little or no supervision, and depend mainly on oneself to get things done
- ANALYTICAL THINKING – Analyze information and use logic to address work or job issues and problems

All employees of the City of Chicago must demonstrate commitment to and compliance with applicable state and federal laws, and City ordinances and rules; the City's Ethics standards; and other City policies and procedures.

The City of Chicago will consider equivalent foreign degrees, accreditations, and credentials in evaluating qualifications.

*May be required at entry.

City of Chicago
Department of Human Resources
December, 2021