



Code: 06E6
Family: IT-Security Analyst
Service: Administrative
Group: Clerical, Accounting, and General Office
Series: Information Technology

CLASS TITLE: SECURITY ANALYST

CHARACTERISTICS OF THE CLASS

Under immediate supervision, the class functions at the entry-level assisting in the administration of IT security services across the City's enterprise network including security analysis, incident response, resiliency, threat management, identity and access management, governance, risk and compliance, network security management, and performs related duties as required.

This class is assigned to the City's Analyst Information Technology Job Family which consists of analysts that work with stakeholders to identify and define needs/issues, document requirements, perform analysis, solve problems with fact-based analysis, and provide recommendations.

ESSENTIAL DUTIES

- Monitors and utilizes intrusion detection systems and security toolsets for the identification of suspicious and malicious activities and inadequate security practices across the City's network (e.g., analyzes network traffic, vulnerability scans, identification of computer viruses, unauthorized user activity) which may compromise the confidentiality, integrity, and availability of systems
- Analyzes and monitors security violations, alerts and reports and acts as a liaison regarding all security vulnerabilities reported.
- Performs security risk assessments, audits and tests against internal sites and systems
- Analyzes, coordinates, and manages threat intelligence data
- Monitors the City's ongoing compliance with regulations, internal policies, standards, and procedures
- Works closely with management and department leaders to ensure business operations requirements meet IT security and compliance practices and policies
- Documents and manages the City's support of identity and access management capabilities
- Develops and coordinates enterprise-wide security training, communication, and outreach efforts
- Manages Information Security projects and issues (e.g., application development/selection, system upgrades and installation, technology initiatives)
- Monitors and reports on enterprise-wide compliance against security requirements
- Collaborates with technology partners, support representatives, and IT management to coordinate and remediate security risks
- Keeps abreast of security related technology, best practices, and regulations
- Prepares technical and status reports for management review
- Functions as a liaison with operating departments IT personnel to ensure City security technology processes and procedures are adhered to (e.g., approval of hardware/software purchases, provide technical expertise and guidance, etc.
- Assists in the development, testing and simulation of the City's continuity of operations and associated plan(s)

- Supports governance, risk, and compliance activities
- Supports activities related to vendor management & contract management, performing appropriate analysis
- Assists with creating and maintaining security policies, standards and procedures
- Performs business analysis including requirements gathering and gap analysis, 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 with an Associate's degree in Computer Science, Cybersecurity, Information Technology/Systems, or a directly related field, plus one (1) year of experience in information security, network architecture or engineering, application development, information technology auditing/compliance or an equivalent combination of education, training and experience.

Licensure, Certification, or Other Qualifications

- Preference may be given to applicants who possess professional IT security, firewall and network certifications

WORKING CONDITIONS

- General office environment
- Stressful situations with imposed deadlines

EQUIPMENT

- Standard office equipment (e.g., phone, printer, copier, computers, mobile devices)
- Standard productivity suites (e.g., Microsoft Office Suite, OpenOffice, Google Workspace)

PHYSICAL REQUIREMENTS

- No specific requirements

KNOWLEDGE, SKILLS, ABILITIES, AND OTHER WORK REQUIREMENTS

Knowledge

Knowledge of:

- *IT and cybersecurity concepts, principles, methods, and practices, in an assigned specialty area
- *information security concepts, toolsets and solutions
- *information system attack methods and vectors
- *incident handling methods and procedures
- *IT metrics, methods, and concepts
- *new and emerging IT security technologies/trends
- *requirement analysis principles and methods
- project management principles, methods, and practices in an assigned specialty area

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

Skills

- ACTIVE LEARNING - Understand the implications of new information for both current and future problem-solving and decision-making
- 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
- COMPLEX PROBLEM SOLVING - Identify complex problems and review related information to develop and evaluate options and implement solutions
- TIME MANAGEMENT - Manage one's own time or the time of others
- COORDINATION WITH OTHERS - Adjust actions in relation to others' actions
- JUDGEMENT AND DECISION MAKING - Consider the relative costs and benefits of potential actions to choose the most appropriate one
- SYSTEMS ANALYSIS - Determine how a system should work and how changes in conditions, operations, and the environment will affect outcomes

Abilities

- COMPREHEND ORAL INFORMATION - Listen to and understand information and ideas presented through spoken words and sentences
- SPEAK - Communicate information and ideas in speaking so others will understand
- COMPREHEND WRITTEN INFORMATION - Read and understand information and ideas presented in writing
- WRITE - Communicate information and ideas in writing so others will understand
- CONCENTRATE - Concentrate on a task over a period of time without being distracted
- RECOGNIZE PROBLEMS - Tell when something is wrong or is likely to go wrong
- REASON TO SOLVE PROBLEMS - Apply general rules to specific problems to produce answers that make sense
- COME UP WITH IDEAS - Come up with a number of ideas about a topic
- MAKE SENSE OF INFORMATION - Quickly make sense of, combine, and organize information into meaningful patterns
- REACH CONCLUSIONS - Combine pieces of information to form general rules or conclusions (includes finding a relationship among seemingly unrelated events)

Additional Competency Requirements

- COMMUNICATION FOR RESULTS – Writes, speaks and presents effectively. Explains the immediate context of the situation, asks questions with follow-ups and solicits advice prior to taking action. Develops presentations to influence others by using graphics, visuals or slides that display information clearly. Listens and asks questions to understand other people's viewpoints.
- GROWTH MINDSET – Takes ownership of personal growth. Identifies knowledge gaps. Asks questions of subject matter experts and seeks help when needed. Keeps abreast of information,

developments and best practices within a field of expertise (e.g., by reading, interacting with others or attending learning events).

- **INITIATIVE** – Volunteers to undertake tasks that stretch his or her capability. Identifies who can provide support and procures their input. Identifies problems and acts to prevent and solve them.
- **OWNERSHIP AND COMMITMENT** – Volunteers to undertake tasks that stretch his or her capability. Checks the scope of responsibilities of self and others. Monitors day-to-day performance and takes corrective action when needed to ensure desired performance is achieved. Identifies problems and acts to prevent and solve them. Identifies who can provide support and procures their input.
- **ANALYTICAL THINKING** – Gathers and links data. Breaks down tasks and problems into manageable components. Reviews for nonconformity and gathers further information in response to routine problems. Solicits guidance as needed to assess importance and urgency.
- **INFORMATION SYSTEMS KNOWLEDGE** – Possesses a basic understanding of the strategy, structures, processes and procedures of the enterprise in its relationship with the business and its activities. Troubleshoots in response to requests for technical support. Identifies problems and needs. Escalates problems to appropriate technical experts.
- **PROBLEM SOLVING** – Issues may not have clearly prescribed solutions and require interpretation of policies or analysis to resolve. Solicits input in gathering data that help identify and differentiate the symptoms and root causes of defined problems. Suggests alternative approaches that meet the needs of the organization, the situation and those involved. Escalates issues with suggestions for further investigation and options for consideration.
- **RISK MANAGEMENT** – Understands the concept of risk, and how this concept can be applied to his or her work.
- **SYSTEMS THINKING** – Seeks advice and guidance on critical linkages between the assigned customer's business, technology and system platforms. Responds to problems by ascertaining the interaction and interdependencies of key system components.
- **THOROUGHNESS** – Performs tasks according to quality and output standards. Takes initiative to ensure that outcomes meet internal and external customer requirements. Solicits feedback on performance of new tasks. Measures accuracy using performance metrics. Sets improvement standards to reduce errors, omissions and oversights.

Other competencies as required for successful performance in the lower-level series.

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.
