Code: 06E4
Family: IT-Engineer
Service: Administrative
Group: Clerical, Accounting, and General Office
Series: Information Technology

CLASS TITLE: SECURITY ENGINEER

CHARACTERISTICS OF THE CLASS

Under supervision, implements and maintains the security measures for the protection of computer systems, networks, and information, in accordance with security policies and guidelines, and performs related duties as required.

This class is assigned to the Engineer Information Technology Job Family which consists of engineers and developers that design, build, test, deploy, and support IT products and solutions.

ESSENTIAL DUTIES

- Creates controls to detect potential security violations and makes recommendations to improve security
- Designs and implements security solutions for detection and notification, security auditing, alerting, and response, vulnerability detection and remediation
- Reviews security information system schematics, diagrams, and other program documentation to assist with development and preparation of cost estimates
- Performs capacity and future growth planning of the enterprise security infrastructure to ensure a highly available security environment
- Verifies security systems by developing and implementing test scripts and running security scans
- Maintains and supports information security tools such as antivirus, end-point detection and response, Data Loss Prevention, vulnerability scanning tools and other security controls which safeguard and monitor events
- Certifies the security functionality of components and services
- Provides expertise and assistance to ensure the infrastructure and information assets are protected
- Validates baseline security configurations for operating systems, applications, networking, and telecommunications equipment
- Participates in 24/7 on-call rotation, Incident Response and Disaster Recovery efforts
- Maximizes security footprint by monitoring security tools, troubleshooting escalated security problems and incidents, identifying security gaps, and evaluating and implementing enhancements
- Provides responsive support for security problems found during normal working hours and outside normal working hours
- Resolves and consults on the most complex security issues and keeps customers informed about security problems and resolutions
- Analyzes reports and historical data to identify security problems and troubleshoots, diagnoses, and resolves security problems
- Communicates status and documents problems and resolutions for future reference
- Assists in the development of incident response, continuity and disaster recovery plans with department stakeholders and third-party service providers

- Evaluates vendor solutions to ensure compliance with requirements and cost-effectiveness, working with vendors to resolve security problems and develop solutions, evaluating services provided and recommending changes
- Develops and maintains enterprise IT standards across the security footprint
- Track, monitors, and analyzes key cybersecurity metrics and KPIs
- Recommends security products by researching needs and evaluating corporate standards list and security training programs targeting specific areas of improvement.

***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 in Computer Science, Information Systems, Cybersecurity or a directly related field, plus two (2) years of work experience in IT and security work, system analysis, application development, systems administration, or designing and deploying security solutions; or an equivalent combination of education, training, and experience.

Licensure, Certification, or Other Qualifications

- Preference may be given to individuals holding one or more Information Security Certifications such as: CompTIA: Security+, GIAC Certification: GCWN, GSEC, ISC2: CISSP, SSCP, CCSP, Cloud Security Alliance: CCSK

WORKING CONDITIONS

- General office environment

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 COMPETENCIES

Knowledge

Moderate knowledge of:

- *designing and implementing security solutions such as network technologies, network monitoring tools, web-related technologies, network/web-related protocols and security solutions supporting Operational Technologies such as Supervisory Control And Data Acquisition (SCADA), Building Controls Systems and Internet of Things (IoT) environments
- *security systems, including firewalls, intrusion detection systems, antivirus software, authentication systems, log management, content filtering, identity and access management solutions, etc.
- *database and operating system security
- leading projects

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.
- BUSINESS FUNCTION KNOWLEDGE – Assesses the needs of primary business functions. Suggests technical solutions for business functions, and implements action plans to improve ongoing business performance in ways that minimize day-to-day disruption of operations.
- 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.
- CONSULTING – Shares information regarding procedures and routine activities. Provides guidance and advice. Suggests caution as appropriate. Asks questions that raise awareness and demonstrate insight.
- INFORMATION SEEKING – Gathers and analyzes information or data on current and future trends of best practice. Uses appropriate tools, techniques and sources to gather, update and monitor information. Checks for accuracy of interpretation. Seeks out the appropriate people for guidance when needed, depending on the type of issue.
- INFORMATION SYSTEMS KNOWLEDGE – Aware of the primary uses of technology by customers, learning the systems of the enterprise and the customers affected. Responds to day-to-day requests for technical support in areas of primary usage. Escalates questions and problems to relevant technical expert groups.
- OUTCOME DRIVEN – Responds quickly and effectively to instructions and requests. Seeks guidance on priorities and goals. Applies effort that is commensurate with the outcome.
- RISK MANAGEMENT – Demonstrates an awareness of the risks involved with working within the organization, makes assessment of the risks of various projects and initiatives, and uses that to mediate his or her own behavior and work.

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.

City of Chicago
Department of Human Resources
March, 2023