Code: 0677
Family: Information Technology
Service: Administrative
Group: Clerical, Accounting and General Office
Series: Information Technology

CLASS TITLE: IT SECURITY SPECIALIST

CHARACTERISTICS OF THE CLASS

Under general supervision, the class functions as a technical expert assisting in the administration of IT security services across the City's enterprise network including security analysis, intrusion detection, incident response, and network security management.

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 integrity and availability of systems.
- Analyzes and monitors security violations, alerts and intrusion detection reports prepared by a third party vendor and acts as a liaison regarding all security vulnerabilities reported.
- Acts as a lead incident handler investigating and mitigating possible security exceptions and incidents (e.g., identify proper investigative approach, conduct interviews, evidence preservation, transportation, computer forensic analysis, and case management).
- Performs complex security risk assessments, audits and tests against internal sites and systems.
- Assists in developing enterprise security strategies, policies and procedures to ensure information system reliability and accessibility (e.g., documentation, notifications, web content, and alerts).
- Manages complex Information Security projects and issues (e.g., application development/selection, system upgrades and installation, technology initiatives).
- Monitors and reports on enterprise wide compliance against vulnerability management requirements.
- Collaborates with technology partners, support representatives, and IT management to coordinate and remediate security vulnerabilities.
- 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 disaster recovery plan.
- 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 or university with a Bachelor's degree in Computer Science, Information Technology/Systems, or a directly related field, plus two years of experience in information security, network architecture or engineering, or application development 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., telephone, printer, photocopier, fax machine, calculator)
- Computers and peripheral equipment (e.g., personal computer, computer terminals, hand-held computers)
- Client/server computers
- Local area/wide area communications network

PHYSICAL REQUIREMENTS

- No specific requirements

KNOWLEDGE, SKILLS, ABILITIES, AND OTHER WORK REQUIREMENTS

Knowledge

Considerable knowledge of:

- *IT concepts, principles, methods and practices, in an assigned specialty area
- *information security toolsets, intrusion detection and response systems
- *information system attack methods and vectors
- * incident handling methods and procedures

Moderate knowledge of:

- *IT metrics, methods and concepts
- *new and emerging IT security technologies/trends
- project management principles, methods and practices in an assigned specialty area
- *requirement analysis principles and methods

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

- *ACTIVE LEARNING - Understand the implications of new information for both current and future problem-solving and decision-making
- *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 and the time of others
- *COORDINATION WITH OTHERS – Adjust actions in relation to others' actions
- *SYSTEMS EVALUATION - Identify measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system
- *QUALITY CONTROL ANALYSIS - Conduct tests and inspections of products, services, or processes to evaluate quality or performance

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
- 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
- DEPENDABILITY - Demonstrate reliability, responsibility, and dependability and fulfill obligations
- ATTENTION TO DETAIL - Pay careful attention to detail and thoroughness in completing work tasks
- INDEPENDENCE – Develop own ways of doing things, guide oneself with little or no supervision, and depend mainly on oneself to get things done
- INNOVATION - Think creatively about alternatives to come up with new ideas for and answers to work-related problems

  ANALYTICAL THINKING - Analyze information and using 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, 2014