## CLASS TITLE:  INFORMATION SECURITY MANAGER

### CHARACTERISTICS OF THE CLASS

Under direction of the Chief Information Security Officer, manages the delivery of IT security services across the City's enterprise network including Network Security, Perimeter Security, Vulnerability Management, Architectural Advice and Incident Handling, and performs related duties as required

### ESSENTIAL DUTIES

- Works with the Chief Information Security Officer as a point person on citywide IT security initiatives as well as the implementation, revision and enforcement of security policies and procedures to ensure information systems reliability and accessibility

- Develops network security architecture for the City, including hardware and software components, Payment Card Industry (PCI) and Health Insurance Portability and Accountability (HIPAA) compliance

- Identifies, investigates and responds to information security incidents reported by client departments and provides post-mortem analysis and recommendations

- Supervises staff responsible for administering IT security services across the City's enterprise network

- Performs quarterly recertification of City's firewall infrastructure configuration and rule base

- Analyzes existing network and firewall architecture against best practices and provides recommendations to ensure alignment

- Oversees and conducts application and network security scans and works with technology teams to develop remediation plans to ensure the protection of data

- Performs security audits, monitors compliance, performs risk and vulnerability assessments of systems and implements processes and methods for addressing non-compliance to information security standards

- Oversees quarterly and yearly security scans required for security best practices (e.g., HIPAA and PCI)

- Identifies foreseeable information security risks in order to comply with privacy and information security policies and procedures

- Reviews and evaluates the impact of changes in software infrastructure that may potentially affect the confidentiality, integrity, and availability of data

- Leads or participates in security meetings with peers and senior management

- Participates in the development, documentation, communication, testing and periodic review and revision of the City's disaster recovery plan

- Participates in the evaluation and selection of security applications and systems and provides technical assistance on the impact that new solutions may have on the enterprise

- Assists in the preparation and management of the security operating budget

- Oversees vendors and other team members on security related projects

- Keeps abreast of security related technology, best practices and regulations
- Prepares project, status and ad hoc reports to keep management abreast of project progress, problems and solutions

*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 five years of experience in information security management and/or network architecture, including three years of project management experience 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 (e.g., CISSP, CISA, CCNA, CCNP, CCIE)
- Preference may be given to applicants who have experience working with ISO27001, NIST 800-53, PCI, and/or HIPPA frameworks

## 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 computer, modems)
- Client/server computers
- Local area/wide area communications network

## PHYSICAL REQUIREMENTS

- No specific requirements

## KNOWLEDGE, SKILLS, ABILITIES, AND OTHER WORK REQUIREMENTS

### Knowledge

Advanced knowledge of:
- *IT security theories, concepts, and practices
- *IT security environment
- *network, operations and protocols (e.g., RIP, IGRP, EIGRP, ISIS, OSPF, and BGP)
- *enterprise architecture models
- *project management methods and concepts

Considerable knowledge of:
- *incident handling and response

- *requirement analysis principles and methods
- *active directory architecture

Moderate knowledge of:

- new and emerging IT security technologies and trends
- virtual computing technologies (e.g., VMware, Citrix)

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
- *LEARNING STRATEGIES - Select and use training/instructional methods and procedures appropriate for the situation when learning or teaching new things
- *MONITORING - Monitor and assess performance of one's self, other individuals, or organizations to make improvements or take corrective action
- *COMPLEX PROBLEM SOLVING - Identify complex problems and review related information to develop and evaluate options and implement solutions
- MANAGEMENT OF PERSONNEL RESOURCES - Motivate, develop, and direct people as they work and identify the best people for the job
- 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
- *EQUIPMENT SELECTION – Determine the kind of tools and equipment needed to do a job
- *OPERATION AND CONTROL – Control operations of equipment or systems

## 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
- 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

**<u>Other Work Requirements</u>**

- INITIATIVE - Demonstrate willingness to take on job challenges

- LEADERSHIP - Demonstrate willingness to lead, take charge, and offer opinions and direction

- 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

- STRESS TOLERANCE – Accept criticism and deal calmly and effectively with high stress situations

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