County of Cook

Human Resources
750 S. Wolcott
Room: G-50
Chicago, IL 60612

COOK COUNTY HEALTH & HOSPITALS SYSTEM
CCHHS

Job Code: 8084
Grade: 24
FLSA: Exempt

STANDARD JOB DESCRIPTION

JOB TITLE
Security Information Officer

DEPARTMENT
Information Systems / Information Technology

Job Summary

The Security Information Officer (SIO) is responsible for leading the development and delivery of a comprehensive information security system for Cook County Health and Hospitals Systems (CCHHS) to protect CCHHS's network security architecture, network access and data from unauthorized access. Leads the development of best practice procedures and standards for information access, security and privacy. Develops and implements risk mitigation strategies to safeguard proprietary information from threats and vulnerabilities. Oversees incident report response planning and investigation into security violations and determines appropriate resolution. Leads the development and delivery of information security awareness programs for employees and other authorized users. And, works with Chief Information Officer – CCHHS to prioritize security initiatives and risk management assessment.

This position is exempt from Career Service under the CCHHS Personnel Rules.

Typical Duties

General Administrative Responsibilities

Management

- Contributes to the management of CCHHS staff and CHHSS' systemic development and success
- Discusses and develops CCHHS system policies and procedures
- Consistently uses independent judgment to identify operational staffing issues and needs and perform the following functions as necessary; hire, transfer, suspend, layoff, recall, promote, discharge, assign, direct or discipline employees pursuant to applicable Collective Bargaining Agreements
- Works with Labor Relations to discern past practice when necessary

Supervision

- Directs and effectuates CCHHS management policies practices
- Accesses and proficiently navigates CCHHS records system to obtain and review information necessary to execute provisions of applicable collective bargaining agreements

Typical Duties (continued)

Collective Bargaining

- Reviews applicable Collective Bargaining Agreements and consults with Labor Relations to generate management proposals
- Participates in collective bargaining negotiations, caucus discussions and working meetings

Discipline

- Documents, recommends and effectuates discipline at all levels
- Works closely with labor relations and/or labor counsel to effectuate and enforce applicable Collective Bargaining Agreements
- Initiates, authorizes and completes disciplinary action pursuant to CCHHS system rules, policies, procedures and provision of applicable Collective Bargaining Agreements

Other Responsibilities

- Directs the information security support and consultation for systems and applications across multiple platforms at all CCHHS locations
- Manage all user access to CCHHS Information Systems and data and revoke access privileges as required
- Provides leadership and guidance on the adequacy of information security measures being developed or utilized with existing and or proposed applications and systems
- Develops and implements security procedures and policies that are in full compliance with statutory and regulatory requirements such as HIPAA. Oversees the dissemination of policies and standards to the CCHHS community
- Develops and implements on going risk assessment programs to maintain security and prevent information breaches
- Recommends methods for vulnerability detection and remediation such as firewall vulnerability testing
- Directs the development and enhancement of Incident Reporting and Response system to address security violations and coordination of resolutions
- Develops information awareness programs for CCHHS employees and authorized users
- Oversees the process to ensure that all users receive periodical IT security training

Reporting Relationship

The Security Information Officer reports to the Chief Information Officer - CCHHS.

Required Minimum Qualifications

- Bachelor's, or higher level degree
- Seven (7) years of experience within an Information Security environment
- Five (5) years management and leadership experience

Preferred Qualifications

- Master's in Business Administration or Master of Science Degree in Computer Science
- Ten (10) years of experience within an Information Security environment
- Three (3) years Information Security experience in a complex healthcare organization

Knowledge, Skills, Abilities and Other Characteristics

- In-depth knowledge of all areas of Information Security, including but are not limited to Mainframe technologies, WEB technologies, Networking technologies, and Distributed Systems technologies (e.g., Firewalls, TCP/IP, PKI based Authentication, UNIX, Window NT, PC/LAN/WAN, VAX)
- Understanding of computer systems characteristics, features, and integration capabilities
- Extensive knowledge of enterprise software applications
- In-depth knowledge of applicable laws and regulations as they relate to technology issues in Healthcare (e.g., HIPAA Privacy and Security, Meaningful Use Initiative, Stark Regulations, etc.)
- Excellent written and oral communications skills
- Proven experience in planning, organization, and development
- Ability to apply technological solutions to business problems
- Ability to analyze and interpret data and workflows effectively, including identification of potential unintended consequences of administrative, policy, and informatics decisions
- Able to work collaborative, innovative, and able to build consensus with physicians, hospital leaders, staff and administrators
- Able to negotiate effectively at all levels. Flexible and able to deal with ambiguity and change

Physical and Environmental Demands

This position functions within a healthcare environment. The incumbent is responsible for adherence to all hospital and department specific safety requirements. This includes but is not limited to the following policies and procedures: complying with Personal Protective Equipment requirements, hand washing and sanitizing practices, complying with department specific engineering and work practice controls and any other work area safety precautions as specified by hospital wide policy and departmental procedures.

Working Conditions and Physical Demands

General office environment where work is generally sedentary in nature, but may require standing and walking for up to 60% of the time. Environment is fast paced and some stress may occur. Visual acumen and manual dexterity for working with computer and keyboards is required.

The above statements are intended to describe the general nature and level of work being performed by people assigned to this classification. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of the personnel so classified.

For purposes of the American with Disabilities Act, "Typical Duties" are essential job functions.

Approval: _____ _____

Donna Hart — Date

Chief Information Officer - CCHHS

Approval: _____ _____

Gladys Lopez — Date

Chief Human Resources Officer