HOSPITAL SECURITY & DATABASE ADMINISTRATOR

DEFINITION

Under general direction, provides security administration and database management for Natividad Medical Center (NMC), in compliance with the Patient Safety and Health Insurance Portability and Accountability (HIPAA) Acts, The Joint Commission (JCAHO) and other regulatory agencies. Primary responsibilities include ongoing oversight and maintenance of information security for the organization to maintain the confidentiality, integrity and availability of all organizational healthcare information systems.

DISTINGUISHING CHARACTERISTICS

The Hospital Security and Database Administrator is a fully experienced journey-level classification, responsible for assisting in the development and implementation of databases and database security policies and procedures, including user log-on and authentication procedures, security auditing procedures and use of firewalls and encryption routines. Incumbent prepares status reports on security matters to develop security risk analysis scenarios and response procedures, as well as performing daily oversight and maintenance of the both the databases and database security processes, practices, and protocols for NMC clinical information systems.

Hospital Security and Database Administrator is differentiated from other Database and Security Administrator-type classes within the County in the nature, focus, diversity, and scope of responsibilities requiring thorough knowledge of the Patient Safety and HIPAA Acts, and of JCAHO regulations, as applied to data systems, clinical and hospital specific software and protocols, knowledge of best practices in the design, development, maintenance and administration of clinical protocols, as well as statistical analysis and reporting, performance measures, performance improvement techniques, and the frequent use of discretion, initiative and independent judgment. Incumbent performs duties as individual contributor, as team leader and/or as project manager, as directed by the NMC Chief Information Officer (CIO) or designee.

Hospital Security and Database Administrator is differentiated from other NMC ISD classifications in that the primary functions are the management of databases and database security.

EXAMPLES OF DUTIES

Nothing in this specification restricts management’s right to assign or reassign duties and responsibilities to this job at any time.

1. Develops, implements and manages multiple databases, such as clinical, admitting, accounting, revenue cycle and supply chain; ensures database integrity.
2. Designs, implements and manages database system security; enforces security policies and procedures through internally controlled self-assessments; assigns and rescinds user accounts; manages user views; assures resource security, enforces password standards, and oversees privileges and permissions; tracks and monitors all database security incidents. Hosts security on multiple platforms including UNIX, Windows and AIX based servers.
3. Monitors and adjusts database management systems and applications; identifies, analyzes, and resolves performance issues.
4. Assures accurate and effective transaction time-stamping, logging and storage; restores functionality following system crashes and other malfunctions; develops backup and recovery job streams; and performs regularly scheduled backups and recovery of databases.
5. Develops system administration procedures and routines that support clinical needs and conform to relevant regulations; establishes information processing requirements and documents data definitions; maps requirements to existing database files.
6. Evaluates, completes, and advises senior management on the approval of security forms (e.g. data use agreements, system assurance questionnaires, certification and accreditation, etc.).

7. Tracks and monitors all database security incidents.
8. Allocates volume and partitions for data stores.
9. Plans and performs security audits throughout NMC to support regulatory compliance as well as internal and external auditing requirements; works with regulatory agencies/groups, to ensure fulfillment of guidelines and requirements.
10. Provides direct support to all staff for security related issues; educates staff about security policies, and consults on security issues regarding user built/managed systems.
11. Identifies opportunities for and contributes to the improvement of quality, safety, and cost, as well as patient and employee satisfaction.
12. Installs and tests new releases patches, and structure changes; and/or coordinates the installation and testing of same, assures proper normalization of data.
13. Actively participates in incident response team.
14. Constructs data flow diagrams and database models into rationalized and normalized physical database forms.
15. Researches and recommends best hardware and software products to support the clinical database, as relates to security.
16. Performs other duties as assigned.

QUALIFICATIONS

A combination of experience, education, and/or training which substantially demonstrates the following knowledge, skills and abilities:

Knowledge and Skills:

Thorough knowledge of:

1. Principles of data architecture, management, analysis, modeling, flow and systems.
2. Methods of data driven application development.
3. Database design principals.
4. Database management systems, utilities and methods.
5. Data warehousing concepts and techniques.
6. Metadata requirements, repository administration, and usage.
7. Networks and TCP/IP including packet inspection.
8. Information protection methodologies and concepts, such as identification and authentication, access control, inception and audit trails.
9. Network security including packet analysis.
10. Web based application and database security.
11. Data security and access control systems, encryption and related matters.
12. System and network exploitation, attack pathologies and intrusion techniques, such as denial of services, Sync attack, malicious code, password cracking, etc.

Working knowledge of:

1. RSA Envision or Network Intelligence experience is required.
2. ISS Siteprotector and related host and network intrusion products.
3. Defense in depth strategies and deployment of security devices.
4. Vulnerability assessments.
5. Intrusion detection/prevention software for Host, Networks and Wireless intrusion.

6. Principles and practices of project management and related software.
7. Firewalls and Security Event Management software.
8. Medical terminology.
9. Hospital administration, processes and procedures.
10. HIPAA, PCI, and other regulations that apply to healthcare and hospital functions.
11. Application systems, network architecture, multiple platforms and new technologies from a security perspective including, but not limited to:
    - Firewalls, Real time Intrusion detection on network and host, Unix, Windows NT/2000/2003, Novell NetWare, networking (switches, routers/protocols), TCP/IP, network services and security vulnerabilities, Network Architecture, DNS, VPN, Application, Database and O/S Security, as well as web-based systems, single sign on, and high level programming languages.
12. Principles and practices of technical (information systems) problem solving.
13. Principles and techniques of software and systems quality assurance and control.
14. Principles, practices, and techniques of providing customer service.
15. Backup and recovery concepts, including disaster recovery.
16. Principles and practices of system security, and database security implementation, monitoring, and enforcement.
17. Principles and practices of software release upgrades, software evaluation techniques, and procedures.
18. Practices and techniques for capacity planning, monitoring, tuning, and maintaining databases.
19. Principles and techniques of analytical computing.

Some knowledge of:

1. Team dynamics and team building.
2. Basic PC helpdesk functions and procedures.

Skill and Ability to:

1. Define organizational data requirements.
2. Define database requirements.
3. Identify and analyze project risks.
4. Work on complex projects that require strong security infrastructure knowledge.
5. Work independently with clients and senior management on information security issues and strategies.
6. Recognize confidential/sensitive issues and maintain confidentiality.
7. Maintain strict confidentiality of data and information processed. Assess risk and take appropriate actions in a timely manner.
8. Incorporate security requirements into hospital network architecture.
9. Work with applications development teams/vendors to identify and mitigate security impacts of application changes, upgrades and implementations.
10. Work with clinical and management staff to understand clinical/business requirements and to facilitate understanding of how technology security tradeoffs influence strategy.
11. Learn and apply new technologies to NMC security infrastructure.
12. Communicate effectively with medical staff, both orally and in writing.
13. Work under pressure, with tight deadlines, and minimal supervision.
14. Take initiative; work independently and in team environment.
15. Effectively analyze, identify, and diagnose data security-related problems and take corrective measures.

REQUIRED CONDITIONS OF EMPLOYMENT

As a condition of employment, the incumbent will be required to:

1. Successfully pass a background investigation.
2. Pass a pre-employment physical/medical assessment.
3. Possess a valid California Class C driver's license. Have and maintain a satisfactory driving record.
4. Perform on-call duties in a 24x7 environment; required to work overtime, irregular hours, variable shifts, evenings, weekends and holidays.
5. *May come in contact with infectious organisms and other potentially hazardous substances.*

EXAMPLES OF EXPERIENCE/EDUCATION/TRAINING

Any combination of training, education and/or experience which provides the knowledge, skills, abilities and required conditions of employment listed above is qualifying. An example of a way these requirements might be acquired is:

Education and Experience:

- Three to five years of experience working with the end user community in a hospital or clinical setting; and
- Coursework leading to a four-year degree in Information Technology with an emphasis in information security; and
- 6-8 years of combined IS and security work with a broad range of exposure to systems analysis, applications development, database design and administration; including 4 years of experience in information security.
- Experience in the development and implementation of appropriate security controls and policies, and the procedures to implement those controls, and identify management tools to monitor compliance.

Licenses and Certifications:

- Certifications such as CISSP, GCIA, MCSE, CISM; and/or
- Industry/Vendor Certifications of a security and storage nature (ISC (2), ISACA, SANS GIAC, SNIA, etc.)

PHYSICAL AND SENSORY REQUIREMENTS

The physical and sensory abilities required for this classification include:

1. Sight sufficient to read computer screens and standard computer printouts.
2. Strength to lift a 30-pound object, without assistance, and items weighing up to 150 pounds with assistance.
3. Manual and finger dexterity sufficient to work with hands in close tolerances and to work with small electronic components.
4. Speech adequate to project voice clearly and adequately to speak in public.
5. Mobility and agility sufficient to bend, stoop and crawl, in order to access computers and servers.
6. Ability to walk and/or stand for 4 hours, such as while conducting training sessions.
7. Ability to remain seated at computer station for extended periods.
8. Hearing adequate to distinguish and identify sounds and voices in a typical office environment.
9. Ability to work around infectious organisms and other potentially hazardous substances.

CLASS HISTORY		**CLASS DATA**	
Class Code:	16E50	Job Group:	03
Established Date:	February 2009	EEO Category:	P
Revised Date:	(New)	Work Comp. Code:	9043
Former Title:	(New)	Bargaining/Employee Unit:	J
		FLSA:	E
		MOCO OT:	N

Prepared by: Gerta McClay, SPHR, IPMA-CP
Management Specialist

Approved by:

/s/ Janine Bouyea
NMC Human Resources Administrator

2/19/2009
Date