SUBJECT: **Physical Security Management Plan**	**REFERENCE NUMBER**: SS-08
	ORIGIN DATE: 9/80
APPROVAL:	**REVISION NUMBER:** 7
	REVISION DATES: 9/80, 11/98, 8/01, 9/04, 2/07, 10/2010, 5/2012, 8/2015
	LAST REVIEWED DATE: 8/2015

PURPOSE
To assure a safe and secure environment for staff, patients and visitors, and to mitigate the risk of loss or damage to corporate property, equipment or infrastructure and injury to persons on [ORGANIZATION] owned or leased properties.

AUTHORITY/ RESPONSIBILITY
Chief Operating Officer
Vice President Real Estate and Support Services
Director, Security

CONTACT/CONTENT EXPERT:
Director, Security

POLICY
The Department of Security provides physical security management for [ORGANIZATION] properties utilizing proprietary personnel and contracted services, departmental programs, physical security systems and other resources.

The specific level and method of security measures necessary at each corporate owned or leased property will be determined by the Security Director in collaboration with [ORGANIZATION] Administration and site management. Facility site security risk assessments are utilized to identify facility and operational strengths and vulnerabilities in order to mitigate risk with physical security measures and/or education and training.

PROCESS

A) Authority and Reporting Relationships

1) The Director of Security is responsible for managing all aspects of the corporate Physical Security Management Plan and works under the general direction of the Vice President of Real Estate and Support Services.
2) The Clinical Operations Team provides support to facilitate the ongoing development and maintenance of the Physical Security Management Plan.
    a) The Clinical Operations Team receives an annual report on chosen activities of the Physical Security Management Plan from the Environment of Care Safety Committee. The Clinical Operations Team will review reports and, as appropriate, will communicate concerns about identified issues and regulatory compliance.
3) Leadership at all levels are responsible for taking an active role in ensuring compliance with the Physical Security Management Plan, as well as identifying and acting upon events or issues in their respective areas which may compromise the overall security of facilities, equipment or infrastructure or the safety of our patients, employees or visitors.
4) [ORGANIZATION] leaders and staff are responsible for learning and following corporate and

departmental Security procedures.

B) Components of Security Management

1) Security Department Policies

a) Security operational protocols and priorities are defined in the Security, Security Operations Management Policy.
   (i) Security staff response to emergency events, and associated polices and protocols, is defined in the Security operations policy.
   (ii) Investigation of criminal activity, suspicious activity, accident and injury and like incidents on [ORGANIZATION] properties is managed through standard practices and dedicated positions within the Security Department, corporate policy defining acceptable behaviors and local, state and federal law.

b) Physical security systems, programs and software, policy and processes are utilized to control access and manage the security of corporate properties, resources, equipment, infrastructure and persons on property.

2) **A physical security presence** is provided in full or in part at specific [ORGANIZATION] properties.

a) Officers are utilized to monitor and maintain the security of [ORGANIZATION] facilities, equipment infrastructure, and individuals.

b) Security Officer staffing is provided to assist and support in routing and emergency situations or events as identified in the Security Operations Management Policy.

c) Contracted officer staffing is provided at specific ambulatory sites where risk assessment has determined minimal presence is beneficial and needed.

d) At properties where a daily physical presence is not provided, the Security Dispatch Center and Security Liaison Officer are available to support and assist site administrators in routine and emergency situations through response and/or verbal direction.

e) Security staff training

   (i) Security Department maintains a dedicated training process and protocols for Security officer and dispatch staff.
   (ii) Dedicated Field Training Officers (FTO's) and the Lead Dispatcher are responsible for accomplishing training of new staff in these roles to assure consistent and thorough training is provided.
   (iii) On-going training is managed via the Security Operations leadership team and conducted regularly throughout the year to assure for updated information and procedure awareness and maintaining required certifications.
   (iv) Training of other Security staff is the responsibility of the leaders of those areas, i.e. Parking, Access/Valet and Security Systems staff.
   (v) Staff are encouraged to establish relationships with professional organizations, such as ASIS, IAHSS and MAHSS, and to explore the professional education and certifications these organizations offer.

3) **Physical security systems** and access control measures, and the associated devices and software, are developed, managed and utilized to provide for physical security of [ORGANIZATION] facilities and persons within; and support authorized access and utilization of facilities and equipment.

a) Developed and managed as defined in the Security, Security Systems and Access Management Policy.

b) Includes, but not limited to, systems such as access control and access card issuance, cameras and video, lock and key hardware, intercoms, duress, burglary, visitor ID systems and associated software.

4) **Operational polices and protocols** within the Security Department, and those supporting organizational response needs, are developed and reviewed regularly with the intent to provide routine and emergency response and support to organizational facilities and staff.

5) **Liaising with public safety agencies** and other health care facilities (HCF)
   a) Security department staff work closely with local, state and federal law enforcement and fire department officials and staff in the routine operation of duties.
   b) Specific liaison work occurs in developing collaborative emergency response procedures and establishing understanding of regulatory requirements.
   c) Security coordinates combined training between local public safety agencies, this department, and other departments and staff within [ORGANIZATION] to establish and maintain awareness, good relationships and understanding of response support services.
   d) Security department administrators and staff communicate regularly with other HCF safety and security teams to establish professional relationships and to identify best practices and community standards.

6) Event Documentation
   a) A dedicated security incident documentation and reporting program is established as defined in the Security Operations Management Policy.
   b) Dispatching and Security events are documented within the security documentation software. If outside agencies are involved in the investigation of an incident, additional reports may be generated.
   c) Release of Security Department records, video or other documentation is restricted.
      (i) Information gathered and maintained by Security Department programs, reports and systems is the property of [ORGANIZATION] and will not be considered public or provided without written request and approval or upon request of legal authority.
      (ii) Information review or release will be requested and approved only through Security Department Administration and related corporate authorities (i.e. Legal Department, Compliance and/or Risk Management.)

7) Identification and Management of Persons on [ORGANIZATION] Properties
   a) A coordinated identification process as defined in the Security Systems and Access Management Policy is in place. Protocols and regulatory requirements are coordinated with various departments, including Human Resources and Compliance & Contracting.
   b) All corporate leaders are responsible for following the [ORGANIZATION] Human Resources policy and assuring enforcement of the staff identification program through education, monitoring of their staff and enforcement of photo identification policy requirements.
      (i) Identification of other authorized persons on property during regular business hours is managed through the [ORGANIZATION] Human Resources policy and required vendor check-in requirements. (Vendors, Contractors, Students, Interns, Volunteers, etc)
      (ii) Visitors and out-patients are managed through routing to appropriate patient areas and scheduling.
   c) Identification of visitors and patients on [ORGANIZATION] property after regular business hours is defined within corporate policy and supported by Security department protocols.
   d) Persons identified as having no business on [ORGANIZATION] properties are managed by Security officer response, support from law enforcement as needed, and a trespass protocol as determined necessary for behavioral compliance.

8) Security Sensitive Areas
   a) Security sensitive areas are defined in the Security Systems policies and special consideration provided to the security of these areas, (including access control and key management policies).
      (i) These areas include Administration, Human Resources, Infant and Child care in-patient units, IT server areas, pharmacies; other areas added as needed and defined by Security and Administration.

b) Security Management will collaborate with leaders of these areas to assure for compliance with regulatory mandates and general practices. These areas are surveyed routinely to assure the appropriate security measures are managed.

9) Emergency Preparedness and Response

a) Collaboration is coordinated with the corporate Emergency Preparedness Manager in development of organizational emergency preparedness and response procedures.
b) The appropriate management and response to security incidents is defined and documented, i.e. infant/child abductions or attempts, missing adult patients, combative or secluded patients, unwanted persons and suspicious activity on [ORGANIZATION] property, severe weather response, incident command management of events, civil disturbances, etc.
c) Corporate leaders are responsible for reviewing their department specific security procedures and systems regularly and reporting to Security any required adaptations or additions.
d) The Director of Security and the Environment of Care Safety Committee are responsible for reviewing the emergency security procedures for sensitive areas annually.

10) **Risk Assessment** in the corporate environment.

a) Security and risk assessments are conducted of facilities, including those in design and construction and remodel plans, and recommendations made to the planning teams prior to finalization, as permitted.
b) The Security Director or delegate will perform a facility risk assessment and analysis prior to final design of new construction, final design of significant remodeling or occupancy changes, or when a new property is acquired, to analyze existing security conditions and determine where mitigation or improvements are required.
c) Recommendations for immediate and planned mitigation are provided to appropriate senior leaders.
d) On both a daily and scheduled basis, risk assessments are accomplished by Security through scheduled and unscheduled Security Officer tours of [ORGANIZATION] facilities. Officers are trained to identify and resolve safety and security risks in the environment. Resolution is through reporting, work order systems or immediate correction.
e) Security staff involved in Lean, Kaizen and root cause analysis events will support the events and conclusions as determined necessary.
f) Security will support facility inspections by external sources as scheduled or required in order to educate and mitigate risks. This includes authorities having jurisdiction, such as the local and state fire marshal, the Joint Commission, CMS, Board of Health, hazardous waste and other such regulatory or voluntary credentialing agencies.
g) Security will support the Environment of Care rounding program by responding, investigating and resolving identified safety or security risks identified.

11) **A Threat Assessment Response** protocol defines a standard process for identifying, investigating and resolving reported threats which have the potential for harm to persons on [ORGANIZATION] properties and/or disruption of business operations and continuity, systems or infrastructure.

12) **Analysis,** debrief or after-action of security incidents and/or facility emergency events are routinely conducted to identify information which may allow for further mitigation of these events through education, process development or systems integration.

13) Vehicular Traffic & Access

a) The Director of Safety and Security is responsible for identifying and controlling vehicular access to facilities and urgent care areas. The following areas have been designated as urgent care areas:
   (i) Hospital Emergency Center
   (ii) Ambulatory Urgent Care Facilities

b) Access to emergency and urgent care units is regulated by roadway directional signs, and managed via ticketing and towing.

14) Orientation and Education

a) [ORGANIZATION] Human Resources Department develops and manages the New Team Member Orientation program for new staff and the on-boarding program development for non-corporate staff, i.e. volunteers, students and interns.
   (i) The security and emergency response procedures introduced during New Team Member Orientation is dictated by this program development. Examples of such information includes: the Security Department roles and location, fire response protocols, and when and how to report incidents or crimes.
   (ii) Orientation content is reviewed and revised as requested or necessary.

b) Specific Programs
   (i) Collaboration with individual department leaders is established to develop content and supporting materials for general and department-specific orientation and continuing education programs.
   (ii) Utilization of this educational information is the responsibility of the department leaders in their department-specific orientation and continuing education programs.

c) Department Leadership Responsibilities
   (i) As defined through Human Resources processes, leaders are responsible for orienting their staff to [ORGANIZATION] security and emergency management programs and policies once New Team Member Orientation is completed and the employee begins their departmental orientation.
      (a) In addition, department leaders of security sensitive areas are responsible for identifying regulatory or mandated security measures required, supporting development and utilization of those measures, and training their personnel in unique or additional security procedures or precautions provided.
      (b) Mandatory training is required annually of staff as part of the continuing education program.
   (ii) Leaders with contracted staff, volunteers, interns, students and like positions are responsible, in collaboration with Human Resources and Compliance, to assure contract language addresses corporate requirements; and an approved orientation program is provided these contractors to assure awareness to [ORGANIZATION] confidentiality and emergency protocols.

15) Performance Improvement

a) Performance improvement standards are established to objectively measure the effectiveness of the Security program.

b) The Director of Safety and Security determines appropriate data sources, data collection methods, data collection intervals, analysis techniques and report formats for the performance improvement standards.