PURPOSE
The purpose of the Security Management Plan is to establish protocols and procedures that assure that a safe and secure environment is maintained for the staff, visitors, and patients of FirstHealth of the Carolinas from harm. Further, it is the focus of the Security Risks Management Plan to protect all property of FHC from theft or vandalism.

The FHC Security Management Plan’s purpose is to provide a program that shall protect employees, patients, and visitors from harm. A risk assessment is conducted to determine the elements of the plan and include all off-site locations. The plan provides processes for the following:

SCOPE
The hospital develops and maintains a written management plan describing the processes it implements to effectively manage the security of patients, staff and other people coming to the hospital’s facilities.

The plan provides processes for the following:

1. FHC identifies a person (s), as designated by leadership, to coordinate the development, implementation, and monitoring of the security management activities.
2. FHC conducts proactive risk assessments that evaluate the potential adverse impact of the external environment and the services provided on the security of patients, staff, and other people coming to the FHC facilities. The potential for workplace violence is considered during the risk assessment.
3. FHC uses the risks identified to select and implement procedures and controls to achieve the lowest potential for adverse impact on security.
4. FHC identifies, as appropriate, patients, staff, and other people entering the FHC facilities.
5. FHC controls access to and egress from restricted/security-sensitive areas, as determined.
6. FHC identifies and implements security procedures that address actions taken in the event of a security incident.
7. FHC identifies and implements security procedures that address handling of an infant or pediatric abduction as applicable.
8. FHC identifies and implements security procedures that address handling of situations involving VIPs or the media.
9. FHC identifies and implements security procedures that address vehicular access to emergency care areas.
10. Reports and investigates all security incidents involving patients, visitors, personnel or property.
11. Establishes emergency security procedures that address:
1. Actions taken in the event of a security incident or failure.
2. Handling of situations involving VIPs or the media.
3. Provision of additional staff to control human and vehicle traffic in and around the environment during disasters.

12. Maintains ongoing monitoring of performance regarding actual potential risks related to one or more of the following:
   1. Monitoring and inspection activities
   2. Emergency and incident reporting.
   3. Inspection, preventive maintenance and testing of equipment.


The scope of the Security Management plan applies to all employees and departments at FHC.

Personnel at off campus facilities are instructed to dial 911 for a security emergency.

As the field of security management is constantly changing, it is understood that these objectives will achieve compliance over time, with revision as appropriate to changes in the healthcare environment.

**ORGANIZATION AND RESPONSIBILITIES**

**EC.01.01.01  EP # 1 & 2**
The hospital identifies a person(s), as designated by leadership, to coordinate the development, implementation, and monitoring of the security management activities.

The President/COO shall appoint a qualified individual to develop, implement, maintain and monitor the Security Management Program, with the title, “Security Manager/designee”. The Security Manager/designee will report directly to the Director of Facilities/designee. The Security Manager/designee is responsible for maintaining a Security Management Program that prepares for and prevents future security incidents by establishing security procedures, in-service orientation and continuing education of all personnel, and monitoring and evaluation of security incidents for opportunities to improve care. The Security Manager/designee is responsible for the day-to-day maintenance of the plan and monitoring and evaluating the security incidents. In-service orientation and continuing education of staff is provided by the Education Department.

The Security Manager/designee is responsible for training of security personnel and maintaining security reports and related documentation. The Safety Committee approves security policies and procedures and addresses security issues as they are identified. All employees are expected to be alert and assist in protecting the safety of patients, staff, visitors, and hospital property.

Directors of departments in conjunction with Security Manager/designee are responsible for orienting new personnel to the department and, as appropriate, to job and task specific security procedures. Department Directors of restricted/security sensitive areas are responsible for training their personnel in any special security procedures or precautions. Where necessary, the Security Manager/designee assists department directors in developing department security programs or policies.
Individual personnel are responsible for learning and following hospital and departmental procedures for security.

The Security Management Program, objectives, scope, performance, and effectiveness shall be evaluated annually by the Security Manager/designee and reported to the Safety Committee.

**GOALS AND OBJECTIVES**

**EC.02.01.01**
The hospital identifies safety and security risks associated with the environment of care. Risks are identified from internal sources such as ongoing monitoring of the environment, results of root cause analyses, results of annual proactive risk assessments of high-risk processes, and from credible external sources such as Sentinel Event Alerts. (See also EC.04.01.01, EP 14; LD.04.04.05, EPs 7, 8, and 10)

FHC conducts a risk assessment annually to determine the elements of the plan and include all off-site locations.

Environmental Tours are conducted to identify actual or potential risks. The following Security Performance Monitors have been established as follows:

A. Patrol the hospital buildings and property to identify and document potential or actual problems.

B. Take appropriate and timely action to prevent crime, injury, or property loss.

C. Establish and maintain security policies and procedures to direct staff performance when responding to security incidents.

D. Provide timely response to emergencies and requests for assistance. Report crime, fire, injury, or other incidents. Communicate externally with local, state, or federal law enforcement and other civil authorities. Provide internal communications, as needed.

E. Control vehicle movement on hospital grounds, including control of parking and access to the Emergency Department.

F. Provide timely response to reports of violent activity or requests for assistance in restraining violent or aggressive patients or visitors.

G. Limit access to the grounds, building, and restricted/security-sensitive areas by enforcement of staff identification policies, and by assisting in the removal of persons from unauthorized areas.

H. Provide timely response to requests for escort, keys and door openings, or other routine requests for assistance.

I. Manage a documentation system for security incidents.

J. Document security department activity; including investigations, routine patrol activity, special and routine requests for assistance, and other activities.
K. Identify problems, failures, and user errors, which require attention and action.

L. Identify performance improvement opportunities.

M. Conduct an annual evaluation of the scope, objectives, performance, and effectiveness of the program

Data from the Performance Indicators are reported at least quarterly to the FHC Safety Committee. Annually, the data from all Environment of Care Performance Indicators is analyzed and prioritized to select at least one recommendation to be made to the leadership of FHC for a performance improvement activity in the Environment of Care.

ELEMENTS OF PERFORMANCE AND INTENT PROCESS

EC.02.01.01
The hospital takes action to minimize or eliminate identified safety and security risks in the physical environment

The security department uses the information from the risk assessments to develop and implement preventative and countermeasures to mitigate security incidents identified with a higher probability of occurring.

A. Security Issues

1. The Security Manager/designee is responsible for identifying security issues involving patients, personnel, visitors, and property and for developing procedures to address them.

2. The Security Manager/designee and individual department heads collaborate on the development of department-specific procedures as needed.

3. Organization-wide security procedures are reviewed and revised at least every three years.

4. A risk assessment is conducted annually, which includes high-risk restricted/security-sensitive areas. Issues concerning security of patients, visitors, staff and property are addressed in the security policies and procedures including patient elopement.

B. Incident Reporting

1. Security incidents are documented and, if outside agencies are involved in the investigation of an incident, additional reports may be generated.

2. The majority of security incident reports are received through a telephone call. After initial response and assessment by Security staff, other appropriate managers/directors may be advised of the incident. Reports of patient and visitor incidents are directed to Risk
Management. Reports of property damage are directed to the Security Manager/designee and Risk Management.

3. The Security Manager/designee is responsible for performing an analysis on security incidents reported to them and for reporting the findings of such analysis to the Safety Committee on, at least, a quarterly basis. The incident analysis is intended to provide an opportunity to identify trends or patterns that can then be used to determine if changes to the Security Program could control or prevent future occurrences.

4. Summary information related to incidents and analysis of such incidents is reported to the Director of Facilities/designee by the Security Manager/designee. Feedback from the analysis of incidents is used by the Security Manager/designee to further develop and improve the Security Program.

5. The incident reporting program is not used to measure Security Program performance because of the unpredictable nature of incident data and the general inability to control variables, such as human behavior. The Security Manager/designee is responsible for managing the security incident-reporting program.

The Security Department works closely with federal and local law enforcement to ensure criminal issues are addressed and proper notification and assistance is rendered.

**EC.02.01.01**

The hospital identifies individuals entering its facilities.

Note: The hospital determines which of those individuals require identification and how to do so.

Hospital identification badges shall be worn by all employees and staff at all times. Electronic systems are in place to control access to restricted/security-sensitive areas through routine security rounds, the use of identification badges, contractor/vendor passes and the card access systems. Security shall be responsible for vehicular and pedestrian traffic control, parking, and the card access systems throughout the facility.

1. The VP of Human Resources and all supervisory personnel are responsible for managing enforcement of the identification program.

2. Human Resources develops policies for identification. All personnel are required to display an identification badge on their upper body while on duty. Identification badges are to be displayed picture side out.

   Personnel who fail to display identification badges are counseled individually by their department director. Recurrent problems with wearing identification badges may result in disciplinary action. Identification badges are not to be displayed unless personnel are on duty. Identification badges are removed from personnel upon termination.

3. The Security Manager/designee is responsible for enforcing visitor identification policies. All contractors and vendors will obtain a pass from the Facilities Department or the Materials Management Department. Visitors will obtain a temporary visitor’s badge at the Emergency Department entrance security desk after hours, and be entered into the Visitor Management System.
4. Patient identification is provided at the unit where patients are first admitted. If a patient’s wristband is damaged, it is replaced by the appropriate staff. Patient identification is not removed upon discharge.

5. The Facilities Department may provide vendor and contractor identification. Identification badges are numbered, controlled, and stored in a locked area.

6. In restricted visitation areas, access is controlled. All other areas have unrestricted visitation, which is controlled by staff observation.

EC.02.01.01
The hospital controls access to and from areas it identifies as restricted/security sensitive as defined by Security policy.

1. The Security Manager/designee is responsible for identifying security sensitive areas.

2. The following areas have been designated as sensitive areas:
   - Pharmacy
   - OR/Surgery
   - Emergency Department
   - Labor & Delivery
   - Behavioral Svs/Psych Unit
   - Medical Records (H.I.M)
   - Intensive Care Unit (ICU)
   - Coronary Care (CCU)
   - Central Energy Plant
   - Telephone Equipment Rooms/Closets
   - Medication Rooms
   - Central Sterile
   - Data Center
   - NICU
3. Personnel assigned to work in sensitive areas receive department level education on special precautions or responses that pertain to their area.

4. FHC controls access to and egress from restricted/security-sensitive areas based on security needs determined as follows:
   - Restricted/security-sensitive areas are addressed ranging from limited access control by use of identification cards and electronic card access systems.
   - General areas are secured using locks and keys and perimeter doors are monitored and recorded.
   - Through departmental policy related to visitor control and clinical staff observation as well as roving security control.

**EC.02.01.01**
The hospital has written procedures to follow in the event of a security incident, including an infant or pediatric abduction

1. The Safety Officer is responsible for coordinating the development of emergency procedures for the Security Program in conjunction with the Security Manager/designee and the disaster sub-committee. The head of each department designated as a security sensitive area is responsible for developing and enforcing department specific emergency security procedures.

2. The Security Manager/designee is responsible for developing organization wide emergency security procedures for handling security incidents or failures, situations involving VIP’s and the media, Infant abductions, and for traffic control during emergencies.


4. Each director is responsible for providing area personnel with an orientation to emergency procedures related to their job. Additional department level training is provided on an as-needed basis.

5. Each Department Director is responsible for reviewing department specific security procedures at least every three (3) years. The Security Manager/designee and the EOC are responsible for reviewing the emergency security procedures for sensitive areas as needed.

6. FHC’S Security management plan provides for additional security staff to control human and vehicular traffic in and around the environment during disasters and vehicular traffic in and around the urgent care areas. This effort is coordinated with the Emergency Management Plan. Additional security personnel also participate in disaster drills.

7. The security department has security procedures addressing the handling of civil disturbances and other situations. These include managing traffic and visitor control.
8. Additional security officers/designees may be provided to control human and vehicle traffic, in and around the environment of care. Security will unlock waiting rooms and make rounds at periodic intervals to maintain a safe and orderly environment. Facilities and security are stationed at entrances, in the Emergency Department, and periodically reports to the Incident Command Center to share information and provide a status report. Security, in conjunction with the Public Relations Department, will assist the media with an acceptable waiting location for information and reporting. Additional officers are called in as necessary to support these functions.

An incident report is completed on all incidents involving patients, visitors, employees or property and forwarded to Risk Management and a report is submitted to the Safety Committee.

An incident includes, but is not limited to:

- Property damage, lost or stolen property.
- Injuries to staff (i.e., injuries to staff caused by patients during assessment and treatment activities).
- Criminal activities
- Theft, pilferage and tampering with medications

**EC 2.10 (8)**
The hospital identifies and implements security procedures that address: Handling of an infant abduction as applicable.

Infant abduction security procedures are implemented to mitigate an incident from occurring. In the event of an incident, the “Code Pink” procedures are put into effect, which secures all exits, and visitors are visually checked upon leaving the facility. A separate FHC Standard Practice, entitled, Code Pink-Infant Abduction covers this issue in detail. This practice is tested at least once annually if population is served.

**EC 02.01.01**
When a security incident occurs, the hospital follows its identified procedures

When a security incident occurs the security department will follow the established and approved standard operating procedures.

**EC 2.10 (9)**
The hospital identifies and implements security procedures that address handling of situations involving VIPs or the media.

There are provisions made for the security of the physical plant, property, patients, visitors, and personnel of FHC during disaster situations. Personnel are trained in the actions to be taken in the event of a security incident.
Any inquiry from the news media will be directed to the Director of Public Relations/designee. Additional security measures will be implemented for the physical protection of high profile patients or those needing additional physical protection (i.e., politicians, entertainers and persons with history of domestic violence.)

FHC shall seek to maintain a cooperative relationship with the news media, which balances the public need for information with the responsibility to safeguard the patient’s right to privacy.

The release of information to the media will be by authorized personnel only.

**EM.02.02.05**
The hospital identifies and implements security procedures that address vehicular access to emergency care areas.

Security will keep the limited Emergency Department parking clear for authorized vehicles only. Security will be on hand for traffic control and will attempt to clear areas of infractions.

Vehicular access to the Emergency Department will be controlled by two (2) security officers/designees in the event of a disaster.

Additional staff will be assigned from the Facilities Management Department and the Personnel Pool to assist the Security Department in controlling vehicular and foot traffic in the event of a disaster. Access to the Emergency area is regulated by roadway barriers, directional signs, and ticketing and towing.

**PERFORMANCE MEASURES FOR 2009**

Performance measures will be utilized to assess the effectiveness of the program’s scope and objectives, and performance elements.

**Performance Measures for 2009:**
- Code Blue Phones functioning properly
  
  **Numerator** - Number of Code Blue phones found functioning properly monthly  
  **Denominator** – Number of Code Blue phones checked daily in one month

- Number of Thefts – Through staff education regarding security of personal items, reduces the amount of thefts to no more than two per month.
- 95% of the staff who can correctly describe FHC’s emergency procedures in case of a security incident or failure.

A final report of the findings is reported through the Management of the Environment of Care Committee, which is forwarded to the Quality Committee and the Medical Executive Board.
ANNUAL EVALUATION OF THE SECURITY MANAGEMENT PLAN'S OBJECTIVES, SCOPE, PERFORMANCE AND EFFECTIVENESS:

The Security Manager/designee will complete an evaluation of the Security Management Plan annually in terms of its objectives, scope, performance and effectiveness. The Environment of Care Functional Team will review the annual evaluation and standards or performance to determine new measures and/or how to make improvement in any standard falling below expectation.

The process for an annual evaluation at FHC functions as follows:

1. The Safety Officer is responsible for coordinating the annual evaluation of the seven functions associated with Management of the Environment of Care. The Security Manager/designee is responsible for performing the annual evaluation of the Security Program.

2. The annual evaluation uses a variety of information sources including the reports from the general liability insurance carrier, internal policy and procedure review, incident report summaries, environmental tour reports, and other summaries of activities. In addition, findings by outside agencies such as accrediting or licensing bodies, or qualified consultants are used. The annual review examines the objectives, scope, performance, and effectiveness of the Security Program. The findings of the annual review are presented in a narrative report supported by relevant data. The report provides a balanced summary of the Security Program performance over the preceding 12 months. Strengths are noted and deficiencies are evaluated to set goals for the next year or longer term future. Representatives from clinical, administrative, and support services participate in the analysis of environment of care data.

3. The annual review is presented to the FHC Safety Committee and other departmental managers as appropriate by the end of the first quarter of each year. The EOC reviews and approves the report. The annual review examines the objectives, scope, performance, and effectiveness of the Security Program. The deliberations, actions and recommendations of the EOC are documented in the minutes. The reports are compiled and sent to hospital administration through the Quality Committee, which reports to the FHC Board. Once the review is finalized, the Security Manager/designee is responsible for implementing the recommendations in the report as part of the performance improvement process. This finalizes the evaluation process.

Approved by the MRH Safety Committee, March 2004
Approved by the MRH Safety Committee, April 2005
Approved by the MRH Safety Committee, March 2006
Approved by the MRH Safety Committee, September 2007
Revised May 2009
Approved FHC Safety Committee 6/10/09
Approved electronically by FHC Safety Committee 1/27/10