THE ENVIRONMENT OF CARE
SECURITY MANANGEMENT PLAN

SCOPE

The Security Management Plan describes the methods of providing security for people, equipment and other material through risk assessment and management for The University of Arizona Medical Center - South Campus, as well as associated off site locations. Security protects individuals and property against harm or loss, including workplace violence, theft, infant abduction, and unrestricted access to medications.

The program is applied to the South Campus and all other associated clinics and off-site areas of The University of Arizona Medical Center - South Campus.

FUNDAMENTALS

A. A visible security presence in the hospital helps reduce crime and increases feelings of security by patients, visitors, and staff.

B. The assessment of risks to identify potential problems is central to reducing crime, injury, and other incidents.

C. Analysis of security incidents provides information to assist with predicting and preventing crime, injury, and other incidents.

D. Training hospital staff is critical to ensuring their appropriate performance. Staff is trained to recognize and report either potential or actual incidents to ensure a timely response.

E. Staff in sensitive areas receive training about the protective measures designed for those areas and their responsibilities to assist in protection of patients, visitors, staff and property.

F. Violence in the workplace awareness; please see UAHN Policy HR-102 Standards of Conduct and Corrective Action.

OBJECTIVES

The Objectives for the Security Management Plan are developed from information gathered during routine and special risk assessment activities, annual evaluation of the previous year's plan activities, performance measures, Security Department Reports and environmental tours. The Objectives for Security to fulfill this Plan are:

- *Conduct and document adequate security rounds on all shifts.*
- *Respond to emergencies and requests for assistance in a timely fashion*

.

- *Maintain and expand current electronic security protection devices, including card access systems, surveillance cameras, and alarm systems.*

ORGANIZATION & RESPONSIBILITY

The Board of Directors receives regular reports of the activities of the Security Management Plan from the Environment of Care Committee, which is responsible for the Physical Environment issues. They review reports and, as appropriate, communicate concerns about identified issues and regulatory compliance. They also provide financial and administrative support to facilitate the ongoing activities of the Security Management Plan.

The Administrator or other designated leader collaborates with the Director of Security to establish operating and capital budgets for the Security Management Plan.

The Director of Security, in collaboration with the committee, is responsible for monitoring all aspects of the Security Management Plan. The Director of Security advises the Committee regarding security issues which may necessitate changes to policies and procedures, orientation or education, or expenditure of funds.

Department leaders are responsible for orienting new staff members to the department and, as appropriate, to job and task specific to security procedures. They are also responsible for the investigation of incidents occurring in their departments. When necessary, the Director of Security provides department heads with assistance in developing department security plans or policies and assists in investigations as necessary.

Individual staff members are responsible for learning and following job and task-specific procedures for secure operations.

PERFORMANCE ACTIVITIES

The performance measurement process is one part of the evaluation of the effectiveness of the Security Management Plan. Performance measures have been established to measure at least one important aspect of the plan.

The performance measures for the plan are:

Security Management Plan Performance Measures

Performance Standard	Performance Indicator	Justification for the Selection of the measure	Source of Data
Security will conduct monthly panic alarm testing for all devices monitored by AMAG or SIS. An alarm should sound and register on appropriate monitoring device.	Percentage of properly working panic alarms. (Needs Improvement: 0-95%, Threshold 96-97%, Target 98-100%)	Staff Safety and Timely Response	Panic Alarm Binder
Security will enforce smoking policy and track number of contacts for non-compliance.	Informational	UAHN Tobacco-Free Environment Policy	Dispatch Log
100% of reported security restraint incidents are evaluated for compliance with established security procedures	% of reports evaluated (0-60% needs improvement, threshold 71-90%, Target 100%)	Assessment incident reporting systems	Security Department Reports
Security arrives within two minutes for emergent patient care and staff requests	% <2 minutes (Needs Improvement: 0-95%, Threshold 96-97%, Target 98-100%)	Assessment of response times	Security Daily Statistics
Security responds to non-emergency Security Presence requests within 15 minutes	% <15 minutes (Needs improvement: 0-79%, Threshold: 89-89%, Target: 90-100%)	Assessment of response times	Security Daily Statistics

PROCESSES FOR MANAGING SECURITY RISKS

Management Plan

The Director of Security develops and maintains the Security Management Plan. The scope, objectives, performance, and effectiveness of the plan are evaluated on an annual basis.

Security Risk Assessment

The Director of Security manages the security risk assessment process for the organization and offsite facilities. The Director of Security is designated to manage risk, coordinate risk reduction activities in the physical environment, collect deficiency information, and disseminate summaries of actions and results. The Director of Security ensures compliance with applicable codes and regulations.

The assessment of the hospital identifies 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 assessment, and from credible external sources such as Sentinel Event Alerts.

The risk assessment is used to evaluate the impact of the environment of care on the ability of the hospital to perform clinical and business activities. The impact may include disruption of normal functions or injury to individuals. The assessment evaluates the risk from a variety of functions, including structure of the environment, the performance of everyday tasks, workplace violence, theft, infant abduction, and unrestricted access to medications.

Use of Risk Assessment Results

Where the identified risks are not appropriately handled, action is taken to eliminate or minimize the risk. The actions may include creating new programs, processes, procedures, or training programs. Monitoring programs may be developed to ensure the risks have been controlled to achieve the lowest potential for adverse impact on the security of patients, staff, and visitors.

Identification Program

The Director of Security coordinates the identification program. All supervisory personnel manage enforcement of the identification program.

Hospital administration maintains policies for identification of patients, staff, visitors, and vendors. All employees are required to display an identification badge on their upper body while on duty. Identification badges are displayed on the individual with the picture showing. Personnel who fail to properly display their identification badge are counseled individually by their department head.

Visitors to patients are not normally expected to have identification. Visitors to some specific units, such as Behavioral Health, are requested to have identification. The Security Officers assist in enforcement of visitor identification policies.

The Purchasing Department provides vendor identification. Contractor identification is provided by Security.

Sensitive Areas

The Director of Security works with leadership to identify security sensitive areas by utilizing risk assessments and analysis of incident reports.

The following areas are currently designated as security sensitive areas:

- ***Cashier's office***
- ***Emergency Services***
- ***Human Resources***
- ***Pediatric Clinic***
- ***Pharmacy***
- ***Behavioral Health Areas***
- ***Other off-site or remote locations***

Personnel are reminded during their annual in-service about those areas of the facility that have been designated as sensitive. Personnel assigned to work in sensitive areas receive department level continuing education on an annual basis that focuses on special precautions or responses that pertain to their area.

Security Incident Procedures

The Director of Security coordinates the development of organization-wide written security policies and procedures, and provides assistance to department heads in development of departmental security procedures, as requested. These policies and procedures include infant and pediatric abduction, workplace violence, and other events that are caused by individuals from either inside or outside the organization. Organization-wide security policies and procedures are distributed to all departments. Department heads are responsible for distribution of department level policies and procedures to their staff and for ensuring enforcement of security policies and procedures. Each staff member is responsible for following security policies and procedures.

Organization-wide and departmental security policies and procedures are reviewed at least every three years. Additional interim reviews may be performed on an as needed basis. The Director of Security coordinates the triennial and interim reviews of organization-wide procedures with department heads and other appropriate staff.

ADM-295 Identification/Access Badges
ADM-280 Searches and Inspections

SAF-700 Safety Program

Security Department Response

Upon notification of a security incident, the Director of Security or designee assesses the situation and implements the appropriate response procedures. The Security Director notifies Administration, if necessary, to obtain additional support. Security incidents that occur in the Emergency Department are managed initially by the Intake Officer in accordance with policies and procedures for that area. The Director of Security is notified about the incident as soon as possible.

Security incidents that occur in the departments are managed according to departmental or facility-wide policy. The Director of Security or designee is notified about any significant incident that occurs in a department as soon as possible. Additional support is provided by the Security Department, as well as public law enforcement if necessary.

Following any security incident, a written “Security Department Report” is completed by the Security Officer responding to the incident. The Report is reviewed by the appropriate Security Supervisor and Director of Security. Any deficiencies identified in the report are corrected.

Evaluating the Management Plan

On an annual basis Director of Security evaluates the scope, objectives, performance, and effectiveness of the Plan to manage the utility system risks to the staff, visitors, and patients.

_____ _____

Ron Coles, Director of Security Date

_____ _____

Sarah Frost, Hospital Administrator Date