


Standard Operating Policy & Procedure		
A-008	Medical Campus Security Policy	
Scope: Medical Campus		
Effective Date: 10/17/1990		Supersedes Policy: N/A
Review/ Revision Date(s): 03/19/1996, 11/13/1998, 11/17/2004, 08/15/2011		
Last Update By: John Pepper		Approved by: Anthony Artrip
	UNIVERSITY OF MIAMI MILLER SCHOOL of MEDICINE	Security Department 1051 NW 14th Street, Suite 145 Miami, FL 33136 (305) 243-7233

Purpose

To set forth general guidelines and practices and establish organizational responsibility for security on the University of Miami School of Medicine campus.

Policy

The University of Miami School of Medicine will provide for the safety and security of employees, students, patients and visitors and protect against the potential loss or destruction of University assets through organizational policies, the assignment of responsibility, the presence of security personnel, and the use of integrated security systems.

Procedures

- 1.0 The Director of Security will oversee security administration and plan and implement security programs and policies.
 - 1.1 Through the establishment of a conspicuous and strategically deployed security force, electronic detection systems, card access system, and the use of photo ID badges, access to University facilities will be controlled and monitored, where appropriate.
- 2.0 Department heads will ensure that good security practices are followed and policies are adhered to at the department level and ensure that specialized departmental security needs are developed and implemented.
- 3.0 Chairs, Directors, Managers, and all other supervisory personnel will ensure that prompt reports are filed with the Department of Security of all actual or suspected losses, thefts, criminal activity, violations of security policy, and any other incidents that could jeopardize the safety or security of University employees, students, patients, visitors, or property.

- 3.1 The Security Department will be responsible for investigating and recommending corrective action where appropriate.
 - 3.2 The Security Department will coordinate these reports with other University administrative departments such as Human Resources, Risk Management, etc.
- 4.0 New employees will receive generic security orientation as part of new employee orientation. However, the department heads will ensure that new employees receive department and job specific security orientation as soon as practical but before employees are expected to function independently. Periodic reviews of such policies are recommended annually.
- 5.0 Employees are responsible for their own personal property as well as that of University property used in the performance of their job. Property, particularly small valuable portable property, should never be left unattended in unlocked areas. Desks, files, cabinets, storage rooms, offices, and other work areas should be locked whenever practical, whenever unattended, and always at the end of the work day. Broken locks and areas which cannot be secured should be reported to your supervisor and/or security for corrective action.
- 6.0 Security Officers are to be on patrol or fixed post duty at all times and will be the principal control source for access to non-public facilities that do not have receptionists, card or telecom access. The Department of Security is responsible for monitoring and responding to problems with the card reader access system.
- 7.0 Through their own activities or from contacts arising from their employment, University employees acquire considerable knowledge, data and information concerning the University's programs and operations. Such information regarding inventions, formulas, policies and plans are considered to be proprietary and confidential and are not to be divulged to outside sources. Department heads and supervisors are responsible for orienting employees about their obligation to protect the security of sensitive University information. For specifics refer to "Employment Agreement" and/or other University non-disclosure agreements.
- 8.0 The Department of Security will issue all new or duplicate employee identification badges and access cards. A digital image of each employee shall be retained by the Department of Security. Only information that can be verified in the University of Miami's Department of Human Resources System (DHRS) will be placed on ID badges. Nicknames will not be placed on badges.
 - 8.1 The Employee Photo Identification Badge will display a photograph, the employee's name, department, and University logo. Access

cards, where required, will be coded for authorized buildings and work hours. This coding must be approved by each department the employee may need access to prior to the Department of Security encoding the card.

- 8.2 The background color of the photograph designates primary employment status of that individual.
 - 8.2.1 BLUE BACKGROUND.....Full Time Regular employee and students.
 - 8.2.2 RED BACKGROUND.....Temporary or Visitor status.
 - 8.2.3 YELLOW BACKGROUND.....Outside contractor personnel.
- 8.3 Security Officers and lobby receptionist will allow entry to non-public facilities only to individuals who possess and display proper identification badges. Visitors and guests must be confirmed with the department they are visiting before entry will be allowed.
 - 8.3.1 All badges must be worn above the waist, with the photo visible at all times while on the Medical Campus premises.
 - 8.3.2 Badges may never be shared or used by anyone other than the person whose name and picture appear on the badge. Employees should never use their badge to provide access for others or expect others to provide access for them.
 - 8.3.3 Employees wishing to enter restricted areas outside their regular scheduled hours must have access via their access card or prior written approval of an authorized manager.
 - 8.3.4 Outside contractors and service people will not be permitted to work after hours or on weekends/holidays unless the person responsible for such work has given the Department of Security advance written notice.
- 8.4 All new employees or employees that need to replace a lost badge, must have an Inter-Departmental Requisition form or pay cash for the replacement fee before the Department of Security can issue the badge.
- 8.5 Access Cards for employees require an Inter-Departmental Requisition form or a \$10.00 cash deposit. Deposits are refunded if and when the access card is returned to the Department of Security. A \$10.00 replacement fee is required for lost access cards.
 - 8.5.1 Temporary employees, visitors and service contractors must give the Department of Security a \$10.00 cash deposit for

photo ID badges, which will be refunded if and when the ID badge is returned.

- 8.6 Should an employee or student lose or forget their Photo ID badge they will be treated as any other visitor or guest.
 - 8.6.1 The employee/student must have other identification, have active employment/enrollment verified through their department, and then be signed like other visitors and guests.
 - 8.6.2 With very few exceptions, the Department of Security Photo ID Section is open from 9:00 a.m. to 12:00 p.m., Monday through Thursday, to take photographs for Photo ID's. The Photo ID Section will be open until 5:00 p.m. on those days so new badges may be picked up. The Photo ID Section is closed on Friday.
- 8.7 Employees/students must promptly report lost or damaged badges and/or access cards to their supervisors so that a replacement badge and/or access card can be issued through the Department of Security. Lost access cards must also be reported immediately to the Department of Security so that card can be invalidated in the computer system. Until an access card has been invalidated it will show the name of the person it was issued to, this means another person could use the card for a wrongful act if they find the card and it was not reported.
- 8.8 Upon termination of employment, the employee's photo ID Badge, and access card if they were issues one, must be returned to the Department of Security prior to release of the employee's final paycheck clearance form.
- 9.0 VISITORS AND SERVICE PERSONNEL:
 - 9.1 Visitors are to enter through designated visitor reception areas only, and must register with the Receptionist or Security Officer. Receptionist or Security Officers will contact the appropriate authorized manager to clear their entry. All former employees must follow this procedure.
 - 9.2 Visitors, friends or relatives of employees will not be allowed in University facilities after hours and on weekends/holidays without Security receiving prior written notification from a department head.
 - 9.3 Children under the age of 16 years old will not be permitted access to any laboratory area or area that stores or uses hazardous materials. Children under the age of 12 years old are not to be left unattended in a vehicle or elsewhere on University property.

- 9.4 With approval of the Department of Security Director, certain and specific outside service personnel and visitors with long term contracts to work on campus, or visiting status, will be issued photo identification badges.
- 9.4.1 Issue of this badge will be highly restricted and such requests will not be granted to most visitors, vendors, and contractors although they may have legitimate need to be on campus frequently.
- 9.5 Individuals who are employed by other University of Miami locations, with true right and need to have frequent need to access Medical Campus facilities may, with the Department of Security Director's approval, will be issued a photo identification badge and access card. Each such request will be handled only on an individual basis.
- 9.6 Employment applicants will be considered as outside guests and, as such, must be escorted at all times while inside campus facilities. Job applicants will not be issued ID badges, but all access not under escort is to be restricted to reception areas.
- 10.0 VEHICLE REGULATIONS:
- 10.1 Speed limit on University property is 15 M.P.H. maximum.
- 10.2 Vehicles must be parked in designated parking spaces.
- 10.2.1 V.I.P. designated parking areas require special permits issued by the Vice Provost's Office.
- 10.2.2 Under no circumstance are employees and/or students to park in posted area for "Visitors", "No Parking", or spaces normally used only for short term pick-up. Reserved spaces in most University parking lots requires pre-payment or is strictly reserved for "visitors." Cars illegally parked in these areas are subject to being towed at the owner's expense.
- 10.2.3 University and personal vehicles must be locked and packages or other similar type objects should not be left in plain view to discourage theft.
- 11.0 PROPERTY PASSES:
- 11.1 Employees, students, contractors, or visitors leaving the premises with cartons, packages, etc., are subject to having these items inspected. All machines, tools, supplies, equipment or related University property being removed from the premises, or being moved from one building to another, must be accompanied by a properly signed Property Pass, which will be retained on file with the Department of Security. The Property Pass must list serial

numbers or other means for providing an accurate description for positive identification by the Department of Security. Personnel who routinely take the same property on/off campus, or who must move it regularly from one building to another, during normal working hours, can be issued a Permanent Property Pass by the Department of Security Director. Permanent Property Passes will be issued on a very limited basis and are valid only during normal working hours.

11.1.1 The authority to sign a Property Pass is limited to the department head, or only those individuals they may specifically designate. Management employees cannot sign their own Property Pass.

11.1.2 Property Passes must also be used for personal items such as radios, calculators, cameras, computers, etc., to help prevent possible loss of personal property left on campus.

12.0 SPECIAL CONDITIONS:

12.1 Supervisors are individually responsible for insuring that all operations are performed with the utmost regard for the safety and security of all personnel involved.

12.2 Employees are expected to cooperate with and adhere to safety and security program rules, regulations and procedures at all times.

12.3 Dishonesty and wrongful acts, of any nature, will not be tolerated. Employees should be aware that it is University policy to seek prosecution for all acts of a criminal nature. Dishonest and wrongful acts are also considered to be grounds for job termination.

13.0 Strict compliance with security regulations is mandatory for all personnel and in instances where individuals consciously or persistently violate such rules, appropriate action will be initiated.