SUBJECT:	Effective Date:	Policy Number:	
Building Access Control	11-16-15	1.16	
	Supersedes:	**Page**	**Of**
	New	1	9
	Responsible Authority:		
	Assistant Vice President, Public Safety		

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to the University community and establishes University protocol for the access and methods of access to University buildings during and after hours. Departments are accountable for costs to secure areas compromised as a result of lost, stolen or unreturned keys. This policy applies to the Boca Raton campus, with partner campuses expected to maintain a similar method of key issuance in coordination with the University's department of Public Safety. This policy does not pertain to Housing and Residential Life, who will maintain a procedure that ensures adequate control over electronic access and physical key control.

POLICY STATEMENT:

Florida Atlantic University strives to provide a secure learning environment while maintaining reasonable use of the campus facilities and protecting the University buildings and contents. The University's department of Public Safety is responsible for the management of the University Master Keying System that controls the production, storage and issuance of keys, the replacement or rekey of lock cylinders, the maintenance of key records, cataloging of and

DEFINITIONS:

Card Access Control System:

Excessive False Alarms: Alarms generated due to misuse of systems which result in an on-site visit by the FAU Police or its representative, and occur in excess of 5 times in any 90-day period of time.

Grand Master Key: Provides total access to all buildings within a particular system on campus. Authorization for this key is granted by the Vice President for Administrative Services or the Assistant Vice President of Public Safety, and is restricted to Public Safety and maintenance personnel only.

Building Master Key: Provides access to all spaces within an individual building with the exception of electrical, mechanical, janitorial, etc. The issuance of this key is restricted to persons authorized by the Physical Plant Director and Vice President of the division in which the employee is employed. Multi-departmental buildings require approval from all affected Director or Dean within their area of responsibility in the building.

Building Sub-Master (Department) Key: Provides access to a group of rooms within a department or building. Authorization for this key will be determined by the Security Access Representative on behalf of the Dean, Director.

Suite Key: Provides access to an individual office as well as the main suite door, supply room or various shared spaces within a department or building. Authorization for this key will be determined by the Security Access Representative on behalf of the Dean, Director.

Individual Room Key: Also referred to as an Operator Level Key: Provides access to a room/office within an individual building. Authorization is granted by the Security Access Representative on behalf of the Dean, Director.

Authorized University Personnel: Pertaining to the issuance of a master key, is someone who requires unrestricted access to the University in performance of his or her duties. This includes, but is not limited to, Public Safety personnel, Facilities Management staff and Environmental Health and Safety.

Owl Card: The official form of identification issued by Florida Atlantic University. Owl cards are issued by Business Services.

Key Fob: An electronic style key used to gain entry to RFID access control systems.

RFID: Radio Frequency Identification, a method of passing a unique number from a key fob, RFID enabled card or other device to the access control system. The number is assigned to a user on the system and cannot be duplicated. Device carries no personal data, and passes only the unique number.

PROCEDURES:

A. Public Safety Responsibilities

1. Create and maintain the University's lock and key system, including codes, standards and service equipment.
2. Maintain a computer-based key management system at the Key Shop.
3. Issue keys with proper authorization and maintain records of same.
4. Maintain a database of all keys, locks, and associated building and room numbers they operate. Maintain database of master key holders and supply various reports to administrators and SAR's such as which keys open what doors under their control.
5. Restore physical security in a timely manner whenever key control has been compromised.
6. Maintain the University access control system server.
7. Provide training and software to any department with buildings under control of the University Access Control system.
8. For users not utilizing the software, Public Safety personnel will complete changes within two business days when requested by an authorized representative in the approved format.

B. Off-Master Keying

1. The University utilizes a master keying system to allow access to classrooms, offices and storage for emergency purposes. Emergencies may be public safety or utility related. Examples include medical, fire, electrical or water line breaks.
2. The University understands the sensitive needs of certain locations due to medical records, experiments or restricted/confidential data. To this effect, the University will allow for electronic access control, which can be restricted to a finite grouping of people, allow for time restrictions and provide an audit log, be used in lieu of the master keying system. This electronic access must be compatible with the currently installed access control program (CCure) and be administered by Security Technology Services.

C. College and Department Responsibilities

1. It is the responsibility of each Dean or Department Director to appoint a Security Access Representative (SAR) and provide a list of buildings and/or room numbers under their control. Each College/Departmental SAR would request key and lock by established procedures for their area of responsibility.
2. Protect keys from loss, theft or unauthorized use. Report lost or stolen keys through the department head to University Police.
3. Any re-key expenses to correct deficiencies in security due to a lost, stolen, misplaced, or unreturned key will be the responsibility of the College or Department.
4. College Deans or Department Directors will be required to authorize building-level master keys within their areas of responsibility. In the event of a shared use facility, all Deans/Directors must agree to the issuance of a building level master key.

D. Security Access Representative Responsibilities

1. Each SAR will submit the requests for their assigned area, and will be treated as the College Dean/Department Designee for issuance of keys for offices, classrooms and suites.

2. SAR will be the point of contact for electronic access to buildings or electronically controlled classrooms.
3. SAR will act as the first level of information for the access control users, ensuring proper usage of the system.
4. Each Department/College shall have two SARs assigned.

E. Key Holders: University Personnel and Students Responsibilities

1. The holder of a key or electronic access to any University facility assumes the responsibility for the safekeeping of the key/card and its use. When leaving a campus area or building, ensure that all doors are secured.
2. Report lost or stolen keys immediately through the appropriate department head to University Police.
3. Prior to leaving the University, all keys must be returned to Public Safety. Departments are responsible for having keys returned on their termination clearance form; prohibiting final checks from being distributed until keys are returned.

F. Key Holders: Contractors, Vendors, and other Non-University Personnel

1. Before keys may be issued to a contractor, the Key Shop requires a curren.0.5(d29.02ed29.02y (

H. Key Issuance

1. Keys will be issued by Public Safety to University personnel in accordance with authorization in this policy.
2. Individuals issued university key(s) will be responsible for the safe keeping and eventual

d) Each department is responsible for the total cost of lock changes and new keys to secure areas compromised by lost keys.

4. Broken or Damaged Keys

a) If a key is broken or otherwise damaged, the Security Access Representative should initiate a key request work order and arrange to have the remaining pieces returned to the Key Shop. If a key is broken off in a lock or is malfunctioning, put in a work order immediately.

b) A new key will be issued after damage verification. There is no charge to exchange the damaged key for a replacement.

K. Annual Inventory

On/about January 1st of each year, Key Shop will develop and send to each department a list of Master Keys that have been issued. Departments using access control will be sent an inventory of staff that have access to their card readers. Users with access to the monitoring software will not be sent an inventory, but instead have access to reports that can be run on demand.

Each Facilities Management department that receives this list shall complete an inventory and certify that all keys are secured and accounted. All master keys issued to personnel must be secured in a locked "key cabinet" within a locked office when not being used by on-duty personnel. No one within Facilities Management's departments will be authorized to carry master keys when not at work.

Inventory/certification must be returned no later than the 31st of the month the inventory issued each year. The Key Shop retains the right to request a physical inspection to actually see all master keys issued to the department.

L. Electronic Access Control and Alarms

4. Classroom or offices that are to be on card access shall have installation done at the expense of the department. To begin the process, submit a Work Order Request and an estimate will be provided.

5. Any building utilizing electronic access control shall have the perimeter door locks changed off the master. The University Police will maintain an emergency override key in the event of catastrophic system failure. No keys to the building will be issued outside of the police department.
6. Authorized Security Access Representatives – A Dean, Director, or Department Head must designate at least one individual, preferably two, within a department to act as the Access Representative from whom STS may accept and process requests for changes to security configurations. Requests for changes not received from the SAR will not be executed.

7. Up-to-Date Security Contact Information Required – It is the department's responsibility to inform STS of changes to contact information for all security services. This includes, but is not limited to, changes in names and contact phone numbers for individuals who should be contacted in the event of security breaches or security service/equipment problems. Contact information must include afterhours contact numbers for at least two individuals per department.

8. Safeguarding of Security Information

    a) Department users of card access, intrusion alarm, and/or CCTV security systems may request information concerning use of systems in their areas through STS. Requests are accepted from the designated Security Access Representative for the areas associated within their department only.
    b) If a request for information is needed as part of an investigation, and requesting the information through the department would jeopardize or otherwise compromise the investigation, the request for information must be sent in writing to STS by the Dean or Director.

9. Alarms generated due to breaches of security are monitored and responded to by the FAU Police Department.

10. Penalty for excessive false alarms. If excessive false alarms are generated by any given area, the FAU Police may:

    a) Require the owner departments to reimburse FAU Police the costs of excessive false alarm responses; and/or

    b) Disarm the alarm.

11. Should the department wish to terminate the Intrusion Alarm or Interior Access Control program in their building, this request must be submitted in writing to STS with a minimum of 30 days' notice. STS will reserve the right to remove all equipment at the termination of agreement.

INITIATING AUTHORITY: Assistant Vice President, Public Safety