Office of the President
University Policy

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 adherence to key system authorizations, and the administration of the Electronic Access Control System. All locks and keys must be authorized by the Assistant Vice President of Public Safety or designee.

University Police and Authorized University Personnel must have unrestricted access to all campus areas for safety, security and health reasons, through the establishment and maintenance of a master keying system. All lock and key work shall be done through Public Safety's key shop. Unauthorized door locks are prohibited; if found, they will be removed and the responsible department/college will be charged with expenses incurred to remove the door locks and/or properly secure the location. Buildings with exterior access control shall be keyed off the master system and keys for the entrances not distributed. University Police will maintain emergency override keys in the event of a catastrophic system failure.

DEFINITIONS:

Card Access Control System: A centrally-managed card access system solution that is installed at approved locations

Intrusion/Burglar Alarm System: A departmentally-localized security system solution that is installed at approved locations and which utilizes local keypad control of arming and disarming through entry of authorization codes.

Security Access Representative (SAR): Assigned by the Dean or Director of the location, this person has the overall responsibility of ensuring that the building users are using the electronic access control system and acts as the Director/Dean's designee for key issuance.

Monitoring Station: A client version of the access control program available for use by the SAR to grant or remove clearances as well as change door times.

Armed State: A programmed state of a security component which allows the generation of an alarm in the event of a security breach.

Disarmed State: A programmed state of a security component which ignores events that may or may not be related to a security breach. While in a disarmed state, no alarms are presented to alarm monitoring stations.

Alarm Shunt: A pre-defined programmable period of time when alarms are NOT sent to the monitoring station due to a legitimate, authorized entry into or exit from an area which is in an armed state

Door Forced Open Condition: A condition which, when a door is armed, generates a security breach alarm to the FAU Police alarm monitoring station. This condition will occur at a monitored door if it is opened without presentation of a valid authorized card; such as through the use of a key or an actual breaking and entering. Reported and uncorrected violations of this and other security policies resulting in unauthorized entries to buildings or false alarms will be investigated and corrective actions taken including, but not limited to, termination of access.

Door Held Open Condition: A condition which, when a door is armed, generates a security breach alarm to the FAU Police alarm monitoring station. This condition will occur at a monitored door if the door is left open for a period which exceeds the programmed alarm shunt time. Reported and uncorrected violations of this and other security policies resulting in unauthorized entries to buildings or false alarms will be investigated and corrective actions taken including, but not limited to, termination of access.

Clearance Codes: Software programming which defines where and when a card may be used to access a given area. Clearance Codes are assigned to individuals based on need as defined by the department, and assignment to a cardholder as requested through a Department Security Authorized Representative.

False Alarms: Alarms which are generated due to misuse of card access systems or intrusion systems rather than by actual security breaches of areas.

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 current signed document on company letterhead with the employees name and position, stating he or she is authorized to check out keys on behalf of that company and that the company is assuming financial responsibility for all re-key required to restore security due to keys lost or not returned. The Construction Project Manager will be responsible for issuance and return of keys.
2. The letter needs to be signed by an appropriate officer of the contractor's company. Loss of keys may require re-key of one or more buildings and the cost is high. The holder of a key to any University facility assumes responsibility for the safekeeping of the key and its use. When leaving a campus area or building ensure that all doors are secured as they were upon arrival. It is understood the key will not be loaned or made available to others.
3. The company’s representative to whom the keys are issued must present picture identification and personally sign for all keys.
4. All keys must be returned to the Key Shop at the completion of project. Written confirmation from the key shop is required before final payment is made by Project Manager.
5. If electronic access to areas is available, keys will not be issued. Construction Project Managers will coordinate with Public Safety to program the vendor/contractor’s card for access. It is the responsibility of the vendor/contractor to obtain an Owl Card at the vendor/contractor’s expense.

G. Keys not issued to a person

1. Keys issued to a department but not an individual person shall have a method to restrict the loss of keys. Keys shall be accounted for by a check-out system set in place by the department.
2. Master keys shall be maintained with the utmost security and be checked in and out by the Security Access Representative for the respective department. Master keys shall not be left unattended in a keybox or able to be taken without being checked out. An alternative is in an electronic locking cabinet, accessible by credential with tracking to determine what keys were accessed, by whom and when they were returned.

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 return of the key(s).
3. The SAR will start a work order indicating the room(s) needing access and the Name and ID Number and contact information of the keyholder.
4. Request for non-master keys will have authorizations verified, key(s) created and delivered to requestor.
5. Building Master and Grand Master Keys issued will be serial-numbered and recorded on issuance. Master keys shall be returned to Public Safety upon termination of employment or transfer to a position no longer requiring master keys.

I. Key Return

1. FAU students, faculty and staff: Return all non-master keys to the Security Access Representative before leaving school, discontinuing employment, changing locations or transferring from your present position. Do not turn keys over to anyone else (such as another person who is assuming your position). You will be held responsible for all keys issued to you. Master Keys shall be returned to public safety, serial number verified and Public Safety shall issue a return receipt for the key and update University databases stating that the master key is no longer in possession of the keyholder.
2. Contractors, Consultants, Vendors, and other Non-University personnel: All keys must be returned to the Key Shop at the completion of project. Written confirmation from the key shop is required before final payment is made.

J. Re-key due to Lost, Stolen, Un-returned & Broken Keys

1. Lost Keys

a) Lost keys are to be reported to the Department Head and University Police.
b) A new key request procedure must be initiated for replacement of keys.
c) Each department is responsible for the total cost of lock changes and new keys to secure areas compromised by lost keys.

2. Stolen Keys

a) If a key is stolen it must be immediately reported to University Police and the appropriate Department Head.
b) A detailed police report must be filed detailing the circumstances of the theft.
c) A new key request procedure must be initiated for replacement of keys.
d) Each department is responsible for the total cost of lock changes and new keys to secure areas compromised by stolen keys.

3. Un-Returned Keys

a) It is the responsibility of the authorizing entity to make every effort to secure keys from personnel terminating employment or students leaving school. If efforts fail to obtain the keys they should be considered lost.
b) Keyholders with keys issued by Public Safety will have a hold placed on final checks or retirement until the key is returned.
c) Students will have a hold placed on their account until all keys are returned.

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

In order to better serve the campus community, the University has one standardized enterprise level access control system. This system has the capability for scheduling door unlocks, allowing card holders with appropriate clearances to enter buildings either afterhours or during set times, and allow for a form of perimeter protection. Departments wishing to supplement with an intrusion detection system may do so within guidelines set forth in this policy.

1. Security System Design Approval – All access control and security system designs must be approved by Security Technology Services (STS). Approval will not be unreasonably withheld.

2. Security System Design Installation – All security system installations, unless granted an exemption by the FAU Public Safety, must be installed and maintained by STS. Exemptions will be granted to use the vendor of record for installations, coordinated through STS and within specifications set forth by FAU Public Safety.

3. All new construction will cover the perimeter entrances to the building with access control and system control doors for access to the building, with a minimum of two readers to enter a space.

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

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: _1.16__

Initiating Authority
Signature: _____ Date: _____
Name: Charles Lowe

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: Elizabeth F. Rubin

President
Signature: _____ Date: _____
Name: Dr. John Kelly

Executed signature pages are available in the Office of the General Counsel