**Access Control for University Buildings and Facilities**

**Policy Statement (R*)**
This access control policy sets the objectives, guiding principles, and operating parameters for the University’s approach to providing access to University facilities while striving for physical security for all occupants and property. This policy addresses critical access needs in a manner to minimize risks associated with protection of the University’s personnel and physical assets. The safety and security of the University’s physical facilities and assets is a shared responsibility of all members of the University community.

**Reason for Policy (O*)**
This policy seeks to achieve the following objectives:
1. Establish effective building security for occupants and property while balancing the ease and convenience of access by employing access control systems.
2. Establish and maintain the integrity and accountability for all access control systems.
3. Establish systems that provide appropriate access to authorized persons to conduct University activity.
4. Establish systems that provide unrestricted access for University Police and select maintenance personnel to all campus areas for reasons of security, safety, and health.

**Scope (O*)**
This policy applies to all FIU-owned campuses and facilities located on the Modesto Maidique Campus (MMC) including the Engineering Center (EC), Biscayne Bay Campus (BBC), Wolfsonian Museum and leased facilities where the University has installed physical key or electronic access control systems. Examples of facilities that currently fall outside the scope of this policy include the Jewish Museum of Florida-FIU, the Miami Beach Urban Studio (MBUS), and FIU @ I75.

The policy does not apply to any FIU building which operates its own independent access system provided that Facilities Management Department (FMD) has approved the use of the system. An example is Student Housing.

This policy applies to all FIU faculty, staff, and students. It also applies to all commercial partners, vendors, contractors, consultants, and all other personnel with authorized access to FIU facilities.

**Definitions (R*)**

Access Control Systems – Refers to both the Electronic Access and or Physical Key Access systems.

Access Manager – Refers to the individual or individuals assigned the responsibility to manage, grant or deny access to a specific room, facility or location.

Electronic Access System – Refers to the electronic system which may be on line or stand-alone that uses the FIU One Card ID.

Physical Key Access System – Refers to the system that uses the traditional metal hard key on doors with or without electronic hardware.

Electronic Access Software – The software or other system used by the Access Manager to assign facility access.
FIU One Card ID – Refers to the official FIU identification card that is used for electronic access.

Key/Access Levels

The following sets forth the various levels for keys and/or access.

1. **Individual Key** – Provides access to a room/office within an individual building. Authorization for this key is granted by the Supervisor and designated Access Manager.
2. **Padlock Key** – Provides access to individual or departmental padlocks. Authorization for this key is granted by the Supervisor.
3. **Building Entry Key** – Provides access to main entry or stairwells to a building. Authorization for this key is granted by the Supervisor and Department Head for their respective spaces.
4. **Department Key** – Provides access to a group of rooms within a department or building. Authorization for this key is granted by the Supervisor and Department Head for their respective spaces.
5. **Telecommunications Key** – Provides access to all telecommunications rooms. Authorization for this key is granted by the Supervisor and Vice President- IT/CIO.
6. **Maintenance Key** – Provides access to all maintenance areas, such as mechanical, electrical, and/or custodial areas. Authorization for this key is granted by the Supervisor, the Department Head and Senior Associate Athletics Director, Dean, Chief Financial Officer, Provost, Athletics Director, or Chief of Staff to the President; for their respective spaces.
7. **Building Master Key** – Provides access to all spaces within an individual building, excluding telecommunications or maintenance areas. A maximum of 3 building masters is allowed, unless approved by exception, as described in the procedures. Authorization for this key is granted by the Supervisor, the Department Head and Senior Associate Athletics Director, Dean, Chief Financial Officer, Provost, Athletics Director, or Chief of Staff to the President; for their respective spaces.
8. **Great Grand Master Key (GGMK)** – Provides total access to all buildings within a particular campus. Authorization for this key is granted by the Supervisor, the FMD AVP or Operations Executive Director, and CFO. Issuance [of the Great Grand Mater Key (GGMK)] is typically restricted to Police Department and maintenance personnel in Key Control. In-depth criminal checks including fingerprinting through the Florida Department of Law Enforcement (FDLE) is required.
9. **Electronic Access** – Provides access to any area that is part of the Electronic Access System using the Electronic Access Software. Certain departments have been delegated authority to manage the assigning of the access to their corresponding areas. Authorization of the access is granted by the Supervisor and designated Access Manager.

**RESPONSIBILITIES (O*)**

1. The FIU Police Department (FIUPD) is responsible for overall campus security.
2. FMD is responsible for the overall management of University access systems and has the lead role in implementing this policy and procedures.
3. Individual key holders are responsible for the safekeeping and eventual return of keys issued to them. An individual key holder is responsible for reporting any lost or damaged key; and is responsible for paying any replacement charge for any lost key or damaged key. Lost or stolen keys will not be replaced until a report has been filed with FIUPD.
4. Individuals are also responsible for using access, whether by physical key or electronic device, in the manner intended when authorized access.

**HISTORY (R*)**

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at [http://policies.fiu.edu/](http://policies.fiu.edu/).
<table>
<thead>
<tr>
<th>Facilities Management</th>
<th>For any questions or comments, the “Document Details” view for this policy online provides complete contact information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Florida International University</td>
<td></td>
</tr>
<tr>
<td>11200 S.W. Eighth Street, CSC 220</td>
<td></td>
</tr>
<tr>
<td>Miami, Florida 33199</td>
<td></td>
</tr>
<tr>
<td>Telephone: (305) 348-4001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FORMS/ONLINE PROCESSES (O*)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key request online process</td>
<td><a href="HTTPS://MYFACILITIES.FIU.EDU">HTTPS://MYFACILITIES.FIU.EDU</a></td>
</tr>
</tbody>
</table>

Links to the above referenced Form(s) available in the "Document Details" Section of the online version of this policy document.

*R = Required  *O = Optional