PURPOSE:

The purpose of this policy is to establish guidelines on the issuance of access to authorized users (employees, students and affiliates) in order to gain entry to certain facilities. This policy is necessary in order to describe specific responsibilities, conditions and practices designed to address critical access needs in a manner which minimizes risks and maximizes the protection of physical assets and private information within the control and/or ownership of the University of Miami (“University”).

POLICY:

The safety and security of the University’s physical space and assets is a shared responsibility of all members of the University community. It is the policy of the University that access to the University’s facilities is controlled in order to prevent and/or limit potential loss. To meet this obligation, the provisions set forth below address the design, administration and management of access control systems and measures to ensure their integrity. Access to the University’s facilities is considered a privilege, and is determined and assigned based on the specific needs and requirements of the University and the user.

DEFINITIONS:

Access shall mean the ability to gain entry into an area, space, and/or facility by means of access device.

Access Devices shall mean all devices and items provided to an authorized user for purposes of providing access. Such access devices may consist of traditional metal key(s), Cane Cards, proximity devices and temporary ID cards, or any electronic means of access (e.g., CBORD and ONITY).

Affiliates shall mean non-employee members of the UM community that include but are not limited to: vendors, volunteers, observers, trustees, members of the citizens’ board, dependents of UM employees, retirees, emeriti faculty, alumni, summer scholars, summer campers, Wellness center members, and tenants (non-UM staff) renting space in a University owned building.
**Building Master Keys** shall mean any combination of electronic card access and traditional metal keys that have access to open multiple doors on the Coral Gables campus. Due to security concerns and the significant cost associated with the loss of a Building Master Key, such keys will only be provided to the individuals listed below upon request after verification from the University’s Police Department:

1. Deans of Schools
2. Chief Administrators (for control of specific areas of responsibility)

**CBORD** shall mean the electronic access technology that allows authorized users to use a Cane Card as the means of gaining access. CBORD replaces traditional keys with an electronic Card reader that is networked into the current Information Technology infrastructure to allow for remote communication. The electronic access readers can be horizontally or vertically swiped. Current standards indicate that CBORD locks are to be used on perimeter doors and in interior spaces where applicable due to high turnover volume, security concerns, main entry to suites and possibly other conditions.

**ONITY** shall mean the electronic locks used to secure interior rooms and facilities, such as mechanical rooms, offices, and other interior spaces that do not have direct access to the building’s exterior. The ONITY system is very much like a hotel access lock, it is a stand-alone, offline lock, and unlike CBORD, it only has the capabilities of being programmed locally at the lock with a hand held programmer, and cannot provide remote lockdown. The ONITY lock or offline electronic lock stores all access history and is maintained in the lock’s memory which requires periodic visits to download/upload information and for battery replacement. ONITY is not designed, nor permitted for installation at doors leading to a building’s exterior.

**ONITY Kiosk** shall mean a stand-alone terminal with specialized hardware and software designed to update University Cane Cards for use with the ONITY locking system.

“**Employee**” shall mean all full-time and part-time faculty and staff members, temporary/casual workers, as well as workers employed on a per diem basis, and student employees.

**Great Grand Master Key** shall mean any combination of electronic card access and traditional metal keys that have access to open **ALL** doors and entry points on the Coral Gables campus. Due to security concerns and the significant cost associated with the loss of a Great Grand Master key, such keys shall only be provided to the individuals listed below upon request after verification from University’s Police Department:

1. President of the University
2. Provost of the University
3. Senior Vice President
4. Associate Vice President, Budget and Planning
5. Vice President for Real Estate and Facilities
6. Chief of Police and delegates
7. Director of Emergency Management
8. Director, Facilities Management Department
9. Facilities Management building managers and managers on-call
10. Access control technicians (i.e., Locksmiths)

**Maintenance Master Key** shall mean any combination of electronic card access and traditional metal keys that have access to open multiple doors on the Coral Gables campus. Due to
security concerns and the significant cost associated with the loss of a Maintenance Master key, such keys shall only be provided to the individuals listed below upon request after verification from University’s Police Department:

(1) Departmental Chief Administrators (for control of specific areas of responsibility)
(2) Zone Leads

**Office Master Keys** shall mean any combination of electronic card access and traditional metal keys that have access to multiple doors within a specific office suite or department space on the Coral Gables campus. Due to security concerns and the significant cost associated with the loss of an Office Master Key, such keys are only distributed to individuals specified by a Dean of a College or School, or a Chief Administrator, and must be approved by the assigned department liaison.

**Power users** shall mean those Building Liaisons and/or Building Administrators who have the ability to provide access to their respective building(s). The designation of power users is based upon the volume of programming changes and building use.

**Residence Keys** shall mean any combination of electronic card access and traditional metal keys that have access to doors within a student’s assigned living area on the Coral Gables campus. Students are only issued access for the building in which they reside and Cane Cards will register invalid when used in another residential colleges/village buildings. Residence Keys are only distributed to the Residential Life Office for issuance to a student, and must be approved by the assigned department liaison.

**PROCEDURE:**

I. **REQUESTS FOR ACCESS AND APPROVAL PROCESS**

A. **REQUESTS GENERALLY**

All requests for access must be made through an approved liaison designated with Facilities Customer Service (“FCS”) and the Access Control Shop. Once a request for access is received via a work order, FCS will process the request, based upon the type of access requested. A person requesting access must meet the applicable criteria as outlined in this section.

1. **EMPLOYEES**

All requests for access for an employee require that the employee have an employee identification number (i.e., C#) and a Cane Card. Once an employee receives their identification number and Cane Card through Human Resources, the employee’s departmental liaison must submit a request/work order at www.miami.edu/sro in order to request activation of the employee’s interior/exterior access. All requests must include employee name, C#, access details (room numbers) and a detailed justification for the type of access sought. In the event a request falls outside of the parameters of a routine request for access, FCS and/or Access Control would request the department liaison submit an account number to be billed for the additional work.

Generally, all routine work, such as the initial provision of access devices, maintenance and repair of access devices will not be considered a billable request. However, in cases where an employee requires access to be reissued due to the loss or theft of an access device, the costs
associated with the new access device will be billed to the requesting department. All non-billable/billable items are subject to review and final determination will be made by the Access Control Lead and/or Manager.

2. STUDENTS

The University's Office of the Registrar is responsible for entering the new student's information into the University's system. The CSGOLD system downloads new information from the University's registration system every night. Once downloading is completed, a new student's card is updated with access to their residence hall building, libraries, pool, and other common areas on the Coral Gables campus.

The University's Office of Housing and Residential Life is responsible for providing access to residential students for their particular living areas. Residential students will only be granted access to their assigned living spaces and their Cane Cards will register invalid if a student attempts to enter a different residential building.

B. TYPES OF ACCESS AND CORRESPONDING APPROVAL

Faculty/staff, students and affiliates may require different types of access. There will be four (4) types of access requests. Each type of request has corresponding approval process, determined by the level of risk and exposure to the University in granting the access. It is the responsibility of all power users to abide by this policy and to adhere to the levels of approval outlined below when providing access to an employee, temporary employee or casual worker.

1. LEVEL 1 ACCESS

Requests at this level seek access to a single door. Such a request is considered the most basic type of access request, and only requires approval from FCS.

2. LEVEL 2 ACCESS

Requests at this level seek access to multiple interior doors with a department, and access to doors leading to the exterior of the building during normal business hours (7:00 am to 7:00 pm, Monday through Friday). Such a request must be reviewed and approved by Access Control Shop before a work order is issued by FCS.

3. LEVEL 3 ACCESS

Requests at this level seek access to: (i) doors leading to the exterior of the building outside of normal business hours; (ii) access to multiple buildings; and/or (iii) access to a single building 24 hours a day/7 days a week. Such a request must be reviewed and approved by the University's Police Department (“UMPD”), and the Access Control Shop before a work order is issued by FCS.

4. LEVEL 4 ACCESS

Requests at this level seek access to: (i) Great Grand Masters; (ii) Grand Masters; (iii) Maintenance Masters; (iv) Building Masters; (v) access to multiple buildings 24 hours a day/7 days a week. Such a request must be reviewed and approved by the Chief of Police of UMPD or his/her designee, and the Access Control Shop before a work order is issued by FCS.
The following flow chart illustrates the various types of access and approvals described above:

C. ACCESS REQUESTED FOR VENDORS AND AFFILIATES

At times, the University's vendors require access to certain facilities in order to render the services for which the vendor has been contracted. The access afforded to vendors will be determined based upon the nature of the service to be rendered. Vendors rendering services on a short-term basis will only be afforded access for a period not to exceed 30 calendar days. While long-term vendors will not have an expiration date for their access, the necessity for continued access will be evaluated either quarterly or bi-annually, as determined by the Access Control Shop. All vendors requiring access to the rooftop of any building must sign in with UMPD during each visit.

II. SEPARATION FROM THE UNIVERSITY; INTER-DEPARTMENT TRANSFERS; LEAVES OF ABSENCE

A. EMPLOYEES
1. **SEPARATION**

Where an employee is separated from the University, it is the responsibility of the immediate supervisor or Human Resources representative to collect all University owned materials including (metal keys, Cane Card, proximity devices, and temporary cards) previously issued to an employee. The department liaison will be expected to: (i) consult with the Access Control Shop to ensure that all devices are accounted for prior to separation; (ii) initiate a work order for the Access Control Shop to terminate all access in the system; and (iii) submit all collected access devices to Access Control within 24 hours of collection, to enable proper and timely deactivation.

2. **TRANSFER**

If an employee is transferring to a new department within the Coral Gables campus, the current department liaison must submit a request to deactivate the employee’s access. The employee’s current liaison is responsible for collecting any keys issued to the employee prior to the effective date of the employee’s to another department. Those keys are to be returned to the Access Control Shop to properly document the return of the keys. The liaison in the new department shall be responsible for requesting access for the transferring employee in the manner described in Section 1 above.

3. **LEAVE OF ABSENCE**

Employees who are on a continuous leave of absence shall be required to submit their access devices to their department liaison prior to the commencement of their leave.

III. **POLICY VIOLATIONS**

Violations of this policy may result in the loss of privileges afforded. Employees determined to have violated this may be subject to disciplinary action up to and including termination of employment. Violations of this policy include, but are not limited to, the following:

- loaning an access device to another individual;
- obtaining and issuing an access device without authorization;
- unauthorized duplication of access devices;
- damaging, tampering, vandalizing, altering or modifying University access devices, hardware; locks or other access mechanisms;
- installing or causing to be installed an unauthorized locking mechanism on University spaces (e.g., offices, labs, etc.);
- Propping doors open to avoid the use of access devices;
- admitting unauthorized person(s) into the building;
- failing to return an access device when requested by the Access Control Shop, UMPD, the issuing department, or upon leaving the employment of the University;
- failing to report missing access devices;
- failing to comply with the request and approval provisions set forth in this policy.
- key boxes are not allowed to be kept within offices and/or departments with University keys. When key boxes are found, they will be relinquished to the Access Control group.