INTRODUCTION

Information Technology staff require physical access to Miller Information Technology as part of their job function. The granting, controlling, and monitoring of the physical access to Information Technology facilities is extremely important to an overall security program. Securing our physical environment and enforcing policies that protect our business information and assets remain critical.

POLICY STATEMENT

The purpose of the Physical Access Security Policy is to establish the rules for granting, controlling, monitoring, and removal of physical access to the Miller Information Technology facilities. The front door and backdoor to MITC 109 and MITC 160 will remain locked at all times. You will need to use your Cardinal Card to access this area. A buzzer is installed to allow the reception desk to grant access to visitors on authorized business. Please assist the reception desk by not allowing visitors to "trail in" behind you, unless they are here to conduct business with you.

- Each Employee of Information Technology is required to wear and make visible their Cardinal Card at all times while present at the Miller Information Technology Center.
- University Employees that are Tenants of Information Technology are also required to wear their Cardinal Card when on premise.
- If you do not have your Cardinal Card, and it is during normal business hours, please go to the reception area of MITC 109 for entrance.
- If you do not have your Cardinal Card, and it is outside of normal business hours*, you will not be granted access to the building. There are no exceptions to this policy.
- Vendors, repair persons or deliveries arriving during normal business hours*, must come to the front desk.
- Only freight deliveries are allowed to be directed to the loading dock and must use the intercom for assistance.
- The identity of the IT staff person must be verified by their access card against the validation list of authorized users list. If they forgot their card their manager must be informed.

<table>
<thead>
<tr>
<th>Information Technology Policies</th>
<th>Effective Date: 06/21/2010 Version: 001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Access Security Policy: 10062101</td>
<td>Revised Date: 07/02/2014 Version: 004</td>
</tr>
</tbody>
</table>

Prepared By: Brenda B. Gombosky,
Executive Director of IT Infrastructure
Physical Security Policy
For Information Technology Miller IT Center

- The validation list of authorized personnel will be reviewed on a monthly basis.
- If vendors, repair persons or deliveries are expected outside of normal business hours*, please provide the HelpDesk with advanced notification to allow entry through the back door. If advanced notification is not provided, the Helpdesk will not allow these persons access to the building. **There are no exceptions to this policy.**
- Visitors (vendors are included in the definition of visitors) to Information Technology are required to wear a visitor’s identification badge.

- Visitors must identify themselves, sign in, and state the individual they have come to see and the purpose of the visit before being granted a visitor’s identification badge and/or a parking permit. They must sign-out upon departure.
- Access to Miller Information Technology facilities must be granted only to Information Technology support personnel, tenants, visitors and contractors, whose job responsibilities require access to the facility.
- The process for granting card and/or key access to the Miller Information Technology facilities must be approved by IT Leadership Team.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the front desk. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be immediately reported to the front desk.
- Individuals, whose card is lost or stolen, must go to the Card Office to obtain a new card. A service charge may be assessed by the Card Office for access cards and/or keys that are lost, stolen or are not returned. Any charges assessed by the Card office will be the responsibility of the cardholder.
- Card access records and visitor logs must be kept for routine review for 12 months.
- Access will be removed when individuals sever their relationship with Information Technology.
- Employees are encouraged to be vigilant and report anyone using unauthorized entrances or suspicious activity immediately.

**DARKROOM ACCESS**
*Unauthorized Persons:

<table>
<thead>
<tr>
<th>Information Technology Policies</th>
<th>Effective Date: 06/21/2010 Version: 001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Access Security Policy: 10062101</td>
<td>Revised Date: 07/02/2014 Version: 004</td>
</tr>
<tr>
<td></td>
<td>Prepared By: Brenda B. Gombosky, Executive Director of IT Infrastructure</td>
</tr>
</tbody>
</table>
Physical Security Policy
For Information Technology Miller IT Center

1. All persons not authorized (this includes Physical Plant and custodial employees) for Dark Room access must be escorted at all times by the Facilities Manager or his backup during both business and non-business hours.
2. They must sign-in and out of the Dark Room; provide a reason and the affected rack number for being in the Dark Room.
3. Sign in sheets must be maintained and uploaded to SharePoint.

Authorized Persons:

1. All authorized persons will have individual key codes to the Dark Room.
2. All server cabinets must be locked.
3. Keys to the server cabinets must be checked-out with Facilities Manager or designated backup.
4. All keys must be signed in and out for accessing the server cabinets and provide a reason and the affected rack number for being in the server cabinet.

RATIONALE

The purpose of this policy

- Facilitate the screening of persons entering the Miller Information Technology Center
- Protect our human resources
- Protect our computing and telecommunications infrastructure within the facility

SCOPE

This policy pertains to all Information Technology employees, tenants, and visitors of Information Technology’s Miller IT Center.

DISCIPLINARY

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers.
Physical Security Policy
For Information Technology Miller IT Center

* Normal business hours are defined as 8:00 AM – 5:00 PM Monday – Friday