Access to Secure Computing Facilities

Original Implementation: July 14, 1998  
Last Revision: April 23, 2013

A secure environment must be maintained for all central computer systems managed by Information Technology Services (ITS). To that end, physical access to all central facilities must be strictly regulated. The process of regulating access will include, but is not limited to, setting guidelines for personnel that will be allowed access, monitoring the physical area for access violations and reporting any suspected violations to the appropriate authorities.

Secure computing facilities at the Boynton Computer Center will be defined as the Boynton Computer Center Machine Room and the adjoining hallway between the east and west entrances to this area containing the report distribution lock boxes.

Guidelines for Access to Secure Facilities

Full Access – The individual will be given keys, door codes, card swipe access, and alarm codes for access to the Boynton Computer Center Machine Room and may enter the facility at will. To be granted full access to secure computing facilities, an individual must meet all the following criteria:

- Have a need for unimpeded access to equipment located within the machine room 24 hours a day, 7 days a week.
- Be employed by Information Technology Services in the operations or technical support areas, or director of ITS.

Limited Access – The individual can be let in to the facility to perform designated tasks that require access to the Boynton Computer Center Machine Room. To be granted limited access to secure computing facilities, an individual must meet all the following criteria:

- Have an occasional need for access to secure computing facilities to perform scheduled maintenance to equipment located within the machine room.
- Be given access to the secure area by a member of the operations or technical support staff.
- Be employed by the university.

Escorted Access – Individual(s) can enter the Boynton Computer Center Machine room only under continuous escort by operations or technical support staff. To be granted escorted access to secure computing facilities, an individual must meet some or all of the following criteria:
- Be a member of a tour group.
- Be a contractor or maintenance person not employed by the university who must perform maintenance, installation, construction, de-installation, or other well-defined task that requires access to the secure area.
- Be accompanied at all times by a member of the operations or technical support staff.

**Report Access** – The individual can be granted swipe card access to the hallway containing the lock boxes, or they can be let in by ITS operations personnel. To be granted report access to the hallway, an individual must meet all of the following criteria:

- The individual must be employed by the university.
- The individual is responsible for retrieving output generated in the computer center on a regular basis.

**General Guidelines for Monitoring Access to Secure Facilities**

Monitoring of the secure computing facilities will be carried out by the operations and technical support staff employed by Information Technology Services. Operations and technical support staff will conduct regular walkthroughs of the facility while on duty. All ITS staff members will report any suspicious or hostile activity to a member of the operations or technical support staff or to the University Police Department (UPD). All individuals granted escorted access to the machine room will sign a log upon entrance. All entrances and exits are video recorded.

Loud or disruptive behavior will not be tolerated in secure areas of the Computer Center. Such behavior detracts from the security monitoring process as well as distracting personnel performing complex tasks in these areas. Individuals or groups engaging in this type of behavior will be asked to leave the area at once; individuals refusing to comply will face disciplinary action. The UPD can enforce this policy.

At all times the hallway doors are locked via magnetic locks. Access to the hallway is logged when access is granted by the card swipe or proximity card reader.

- **Business Hours** - During the hours of 8 a.m. - 5 p.m., Monday through Friday excluding holidays, the east and west entrances to the secure area will grant access via the magnetic card readers to individuals with Full Access, Limited Access, and Report Access. In addition, the east entrance to the Boynton Building at the corner of Aikman and East College will be unlocked during this same period. During these periods, operations and technical support staff will regularly check that the doors to the machine room are closed and locked, and that no unauthorized individuals are in the Machine Room.
- **Off Hours** - Any time other than normal business hours, access to the secure area is only permitted to individuals with Full Access. In addition, the east entrance to the Boynton Building at the corner of Aikman and East College will be closed and locked.

**Guidelines for Reporting Suspected Violations**

During normal business hours, the person discovering an access violation will immediately report it to the director or the assistant director of ITS. The University Police Department (UPD) will then be notified at once by one of these individuals. In the event the director or assistant director of ITS is not available, the person discovering the violation will contact UPD immediately.

During off-hours, the security alarm is monitored by UPD. If the alarm is triggered, UPD will contact the appropriate personnel provided on the emergency contact list. The contact person can then assess the situation and advise the assistant director, director of ITS and others as needed. In the absence of the assistant director, the systems manager or systems programmers may be called to initiate action.

At any time one of the contacts can initiate the disaster recovery plan if the situation includes damage or potential further damage to the computer center that would impact normal operations. Under no circumstances should a staff member confront individual(s) committing an access violation that might even remotely be considered a threat. Staff will move to a safe location and call UPD at once. The Department of Audit Services will be notified in writing within 24 hours of any access violation.

**Cross Reference:** 1 Tex. Admin. Code § 202.73

**Responsible for Implementation:** Provost and Vice President for Academic Affairs

**Contact for Revision:** Director of Information Technology Services

**Forms:** None

**Board Committee Assignment:** Building and Grounds