Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.27	**Physical Security for Information Resources**	Responsibility:	Chief Information Security Officer

PHYSICAL SECURITY FOR INFORMATION RESOURCES

Policy

All Information Resources must be physically protected based on risk.

Security controls must incorporate policies, standards and procedures for:

1. Protecting facilities in proportion to the criticality or importance of their function, the classification of data stored, transmitted or access by the Information Resource and the confidentiality of any Information Resources affected;

2. Managing access cards, badges, and/or keys;

3. Granting, changing and/or removing physical access to facilities to reflect changes in an individual's role or employment status; and

4. Controlling visitor and vendor physical access with procedures that incorporate the following:

    a. advanced scheduling, logging and documenting of visits;

    b. escorting while on premises; and

    c. restricting the unauthorized use of photographic and video devices while on premises.

All Data Centers, Master/Main and Independent Distribution Facilities and Telecom Rooms must incorporate each of the following additional security controls:

1. Centrally managed access control system installed on all access points;

2. No externally facing windows;

3. Reviewing physical access semi-annually, or more often if warranted by risk;

4. Designating staff who will have authorized access during an emergency;

5. Monitoring the exterior and interior of the facility 24/7 by trained staff;

6. Maintaining appropriate environmental controls such as alarms that monitor heat and humidity, fire suppression and detection systems supported by an independent energy source and uninterruptable power systems capable of supporting all computing devices in the event of a primary power system failure; and

7. Electronic alarms for all entry points into the facility.

Accountability

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, "*Handbook of Operating Procedures*".

References

- U.T. System Policy 165 Standard 16