## UTEP Standard 16: Data Center Security

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their job function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program. The following is to establish the rules for granting, monitoring, control, and removal of physical access to Information Resources facilities.

16.1 Protection. All Information Resources must be physically protected based on Risk.

16.2 Safeguards. The University has adopted safeguards to ensure appropriate granting, controlling, and monitoring of physical access. Physical access safeguards incorporate the following Procedures:

(a) physically protecting all Information Resources facilities must be in proportion to the criticality or importance of their function and the Confidentiality of any Information Resources affected. Additionally, all physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes;

(b) managing access cards, badges, and/or keys:

i. request must include the approval of the person responsible for the facility,

ii. must be documented and managed,

iii. requests for access must come from the applicable UTEP Data/System Owner,

iv. each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and Non-Disclosure Agreements and/or Acceptable Use of Information Resources and Security Policy Agreement,

v. access cards, badges, and/or keys must not be shared or loaned to others,

vi. access cards, badges, and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process,

vii. lost or stolen access cards, badges, and/or keys must be reported to the person responsible for the Information Resources facility,

viii. card access and visitor logs records for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected,

ix. the person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access,

x. a service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned, and

xi. signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed;

(c) granting, changing, and/or removing physical access to facilities to reflect changes in an individual's role or employment status:

i. access to Information Resources facilities must be granted only to UTEP support personnel and contractors, whose job responsibilities require access to that facility,

ii. the person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within UTEP or are separated from their relationship with UTEP, and

iii. the person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access;

(d) controlling visitor and Vendor physical access:

i. all Information Resources facilities that allow access to visitors will document and track visitor access with a sign in/out log,

ii. visitors must be escorted in card access controlled areas of Information Resources facilities, and

iii. unauthorized use of photographic and video devices while on premises is strictly prohibited without prior authorization.

16.3 Central IT Managed Data Centers and U.T. System Shared Data Centers. In addition to the controls required in Standard 16.2, Data Centers managed by Institutional Central IT organizations and the U.T. System

Shared Data Centers, the person responsible for the Information Resources facility must adhere to the following:

(a) review physical access on an as needed basis;

(b) designate staff who will have authorized access during an emergency;

(c) maintain 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;

(d) protect any Shared or Central IT Managed Data Center built after the effective date of this Standard by implementing and maintaining the following:

i. security fencing, lighting, and landscaping to prevent concealment of intruders,

ii. electronic alarms for all entry points into the facility and any internal areas housing critical infrastructure, and

iii. computer rooms with no externally facing windows;

(e) perform and document a risk assessment on an as needed basis to insure appropriate controls, based on Risk, to protect the state's Information Resources from unauthorized modification, deletion, or disclosure by Owners of Mission Critical Information Resources and Information Resources containing Confidential Data in accordance with Standard 10 – Risk Management. Controls shall extend to Information Resources outsourced by the University; and

(f) a System Information Form must be submitted to the CISO for servers that are physically located in the Central IT Managed Data Center within the University Enterprise Computing Group and the information must be kept up-to-date.

16.4 Decentralized IT Managed Data Centers. In addition to the controls required in Standard 16.2, the ISO shall develop Institutional Standards and safeguards to protect Decentralized IT Data Centers based on Risk.

16.5 Revision History

First Draft: May 30, 2017
Approved: June 9, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer