UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: PS0002.02	Category: Physical Security	Version Date: 02/22/2010
Title: **Physical Security of Server Rooms**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 12/04/2009
Review Resp: HSC Chief, Information Security		Next Review: 12/04/2012

Purpose:

To establish standard physical security requirements for rooms that house servers. A server is defined as "a system entity that provides a service in response to requests from other system entities called clients". For purposes of this standard, minicomputers and mainframe computers are among the equipment considered as servers.

References:

1. SPICE Standard GP0003.02: Information Classification.
2. Policy PS0002: Physical Security of Information Assets and Related Facilities.
3. UF Division of Environmental Health and Safety Requirements
   http://www.ehs.ufl.edu/General/default.asp
4. UF Physical Plant Division Key and Lock Policy
   http://www.ppd.ufl.edu/pdf/Key_Lock_Policy.pdf
5. UF Telecommunications Construction Standards
   http://telecom.cns.ufl.edu/ConstructionInfo
6. UF Telecommunications Construction Standards:
   Appendix #1: UF Network Services Labeling and Naming Conventions.

Standard:

1. Server rooms that house Restricted, Sensitive, or Operational information shall be secured according to the following standards. If the classification of information being housed cannot be determined, the highest level of security controls will apply:

	Restricted/Sensitive	Operational
Access	• New or refurbished server rooms will be locked at all times using an auditable and programmable locking mechanism capable of being monitored remotely. • Access to the server room will be restricted by key, code, or electronic card. An auditable process for issuing keys, codes, and/or cards	• The Unit ISM will maintain a list of all personnel having access. • If used, keys will be stamped "Do Not Duplicate". • If access codes are used they will be changed at least every 6 months.

	shall be documented. If used, keys shall be stamped "Do Not Duplicate". • If access codes are used they will be changed at least every 6 months. • The Unit ISM shall maintain a list of all personnel having access. • Means of entry shall be provided on a strict "need to have" basis as determined by the Unit ISM and approved by the Unit ISA. • Guests will be required to sign a guest log and be escorted at all times.	
Usage	• There shall be no eating, drinking, or smoking allowed in the server room at any time.	• There shall be no eating, drinking, or smoking allowed in the server room at any time.
Physical Safeguards	• Server Rooms shall meet the Florida Building Code as enforced by UF Division of Environmental Health and Safety. • Servers shall be located in a room designed for housing server computers and ancillary equipment (Secured Server Room managed by a Unit ISM). Such room shall be totally enclosed and physically separate from space designed for any other purpose and have appropriate environmental and fire/water hazard detection/suppression/prevention controls. • Provision for staff to perform server operations may be located within the server room. • Wiring shall be routed in Server Room away from personnel working areas and in a manner that allows for cable identification and maintenance. • There shall be no external signs making the server room	• Server Rooms shall meet the Florida Building Code as enforced by UF Division of Environmental Health and Safety. • Wiring shall be routed in Server Room away from personnel working areas and in a manner that allows for cable identification and maintenance. • There shall be no external signs making the server room identifiable • All detection and monitoring devices shall be tested on a regular basis as recommended by the manufacturer. Fire suppression must be tested in compliance with State Fire Marshall requirements and in a manner that does not disrupt operations. The occurrence of testing shall be documented. • Cleaning supplies shall not be stored in the server room.

	identifiable. • Display devices shall be located so that the information displayed is not visible from outside the room. • All detection and monitoring devices shall be tested on a regular basis as recommended by the manufacturer. Fire suppression must be tested in compliance with State Fire Marshall requirements and in a manner that does not disrupt operations. The occurrence of testing shall be documented. • Cleaning supplies shall not be stored in the server room.	
Record Keeping	• Documentation of all repairs and modifications to the physical components related to security (*e.g.*, doors, hardware, locks) shall be maintained for a period of six years.	
Contingency	• A sufficient uninterruptible power supply shall be in place and be of sufficient capacity to enable a normal shutdown in the event of power failure. • A backup plan shall exist in case of an air-conditioning failure. • Provision shall be made for physical access in support of restoration of services and data by authorized personnel in the event of a disaster.	

2. The Unit ISA and ISM shall set the standards for facilities that house <u>only</u> unrestricted information.

Guidelines:

1. The following guidelines are suggested in addition to the above standards:

	Restricted/Sensitive	Operational
Access	• Server rooms should be locked at all times using a multi-factor access control system capable of being	• The server room should be locked at all times. • Guests should be required to sign a

	audited and monitored remotely. • The guest log and the access log should be reviewed by the Unit ISM at least monthly.	guest log. • The guest log and the access log, if any, should be reviewed by the Unit ISM at least monthly.
Physical Safeguards	• There should be no windows from the outside of the building. • There should be at least one fire alarm inside and one outside the server room monitored by Physical Plant. • The water and smoke detectors should be monitored by Physical Plant. • Emergency power-off switches should be inside the server room. Switches may be placed outside the server room if adequately secured. • The room should be above the entry level of the building. • Provision for surveillance of entry points and the server room should be made. • A pre-action, dry pipe suppression system should be in place. • An electronics-safe fire extinguisher should be prominently located inside the server room.	• There should be at least one fire alarm inside and one outside the server room. • The fire department should conduct inspections on a regular basis. • Emergency power-off switches should be placed both inside and outside the server room. In the case of an emergency, systems should be able to be shutdown quickly to prevent significant data loss. • A backup plan should exist in case of an air-conditioning failure. • An electronics-safe fire extinguisher should be prominently located inside the server room.