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

Purpose:

To establish standard physical security requirements for communications closets. A communications closet is a room that houses communications equipment such as routers, switches, hubs, punch down blocks, and other equipment used to support electronic communications.

References:

1. Policy PS0002: Physical Security of Information Assets and Related Facilities.
2. University of Florida Telecommunication Standards http://telecom.cns.ufl.edu/ConstructionInfo

Standard:

1. Access:
    a. Entry to a communications closet shall be restricted to personnel having responsibility for installing or maintaining the equipment in the communications closet. Others requiring access shall be escorted by authorized personnel.
    b. Access to communications closets shall be restricted by key, code, or electronic card. An auditable process for issuing keys, codes, and/or cards shall be documented. All keys shall be stamped "DO NOT DUPLICATE".
    c. Access codes, if used, shall be changed every 6 months.
2. Usage:
    a. A communications closet may be shared with telephony equipment.
    b. New or refurbished communications closets shall not be shared with electrical service or unrelated services.
    c. If not feasible to avoid sharing of current communications closets, communications equipment shall be housed in a locked box appropriate to the purpose or segregated by fencing. Appropriate access controls shall be used.
    d. Communications closets shall not be used for storage.
    e. Communications closets shall not be used as a "pass through" to another room.

3. Physical safeguards:
    a. Communications closets will be constructed to meet the referenced University of Florida Telecommunication Standards.
    b. Door or cabinet hinges should:
        i. Face the inside of the closet if feasible, or
        ii. Have the hinge pin secured (spot welded or other means).
    c. Doors should not have intake grills. If necessary for ventilation, grills shall be installed so that they cannot be removed from the outside of the door.
    d. All detection and monitoring systems shall be tested on a regular basis as recommended by the manufacturer, and the occurrence of the tests documented. Fire suppression must be tested in compliance with State Fire Marshall requirements and in a manner that does not disrupt operations. All detection and monitoring devices shall alert the appropriate personnel.
    e. Uninterruptible Power Systems (UPS) with built in surge protection shall be installed.
    f. UPS systems shall be tested on a schedule recommended by the manufacturer and the occurrence of the tests documented.
    g. A backup plan shall exist in case of an air conditioning failure for those closets that are air-conditioned.
    h. There shall be no eating, drinking, or use of tobacco products allowed in the communications closets at any time.
4. Maintenance Records:
    a. Documentation of all repairs and modifications to the physical components that are related to security (*e. g.*, doors, hardware, locks) shall be maintained for a period of six years.

Guidelines:

1. The following guidelines are suggested in addition to the above standards:
    a. Communications closets should not have windows.
    b. Water detectors and related infrastructure should be placed in the closet.
    c. There should be no external signs making the Communications Closets identifiable.