Physical Access to Sensitive Data Systems

Date: 06/09/06	**Policy ID:** UVAW – 8	**Status:** Approved

Contact Office: Department of Information Technology

Oversight Executive: Director of Information Technology

Applies to: UVa-Wise Campus and Networks

Reason for Policy: Layered protection of data and resources is an accepted best practice. By limiting physical access to computing resources such as servers, switches, routers, etc. another layer of protection is added.

Definitions:

Policy Statement: Physical access to sensitive data will be restricted. Limiting access will provide necessary controls to help ensure the confidentiality, integrity and availability of data and resources needed to fulfill the mission of the College.

Procedures:

1.0 Physical Access to Sensitive Data is restricted
- 1.1 Access to systems that store, process, and/or transmit sensitive data must have appropriate facility entry controls, such as locked windows, doors and/or cabinets.
- 1.2 Unused network jacks on the same network/subnet as systems with sensitive data shall be disabled.
  - 1.2.1 Enabling these jacks should only take place when needed and should not be assigned IP addresses via DHCP but shall be assigned a static IP address.
  - 1.2.2 Visitors in these areas shall be restricted.
- 1.3 Access cards and/or keys to restricted areas should only be given out by OIT Directors.
- 1.4 Visitors i.e. vendors, etc. shall sign into a visitor's log with the following information: date, time, reason for visit and the responsible OIT staffer's name

2.0 Media, including but not limited to paper, electronic, and backups, containing sensitive data must be stored in a physically secure location at all times.
- 2.1 Media, including but not limited to paper, electronic, and backups, containing sensitive data must be properly labeled as confidential and be properly inventoried.

3.0 All records should be retained in accordance with the College policy on records retention and disposition, University of Virginia record retention policy, UVAW-16 Computer – Hard Drive Disposal Policy and the code of Virginia. Records that are retained by an individual, even if they are retained on an electronic medium, are subject to the Virginia Freedom of Information Act and the Privacy Act.

3.1 Media, including but not limited to paper, electronic, and backups, containing sensitive data must be properly destroyed when no longer needed.

3.1.1 Paper media shall be shredded with a cross-cut shredder.

3.1.2 Electronic media shall be physically destroyed (see UVAW-16).

Related Information: See also: UVAW-16 Computer – Hard Drive Disposal Policy; Limiting Physical Access Policy PCI – 9; University of Virginia record retention policy.

Background: Approved by Brian Ward, CIO – UVa-Wise, June 13, 2006
Revision: To update "Related Information", 08/23/19
