Name of Standard: Data Closet Access and Change Control.

Standard Number: TBD

Approving Officer: Director, Network Services and Information Security Officer

Responsible Agents: Networking and Information Security offices.

Scope: all University campuses

| X | New standard proposal | ☐ | Minor/technical revision of existing standard |
| ☐ | Major revision of existing standard | ☐ | Reaffirmation of existing standard |

(A) Purpose

This standard is intended to mitigate risk to the University’s computing infrastructure due to undocumented modifications made to information technology network equipment and infrastructure.

(B) Associated Policies

Network and Telecommunications Policy; 3364-65-09.
Data Center / Data Closet Access Policy; 3364-65-10.

(C) Standard

1. Data Closet Access / Change Control Logs will be posted in all Information Technology data closets. Critical data closets will be equipped with electronic access controls with monitoring capability as resources allow.
2. Personnel accessing data closets will annotate access on the Data Closet Access / Change Control Log and annotate any changes made to Information Technology network equipment or infrastructure located in the data closet.
3. Information Technology Networking and/or Security office will periodically verify data closet access logs.
4. Failure to properly follow data closet access and change control processes may lead to disciplinary action or loss of access.

Approved by:

//approved// ____________________
Robert Hogle
Director of Network Services and Information Security Officer

May 26, 2011 ________________

Date

Review/Revision Completed by:

Director of Network Services

Standards Superseded by This Standard: None

Initial effective date: May 26, 2011
Review/Revision Date: N/A
Next review date: May 26, 2014