SECURING AGAINST UNAUTHORIZED PHYSICAL ACCESS PROCEDURES

Related Board of Trustees Policy:
Approval:
Revision:
NC Statewide Technology Standards (ed. August, 2010 Corrections): 20107, 20108

Securing Against Unauthorized Physical Access

Purpose: To protect the College's information technology assets with appropriate physical controls.

Physical access to areas housing information technology assets is appropriately controlled. Authorized individuals may include College employees, contractors and vendors. A login and logout is required for access for all rooms shall be maintained.

Restricting Access

Information technology assets will remain behind locked and secured areas specifically designated for those assets such as wire closets and datacenters. Datacenters will have their own dedicated door with a mechanical or electronic lock that only authorized individuals have the access code to. IT common areas will also be protected by a locked door that is to remain closed at all times. Datacenters will contain video camera systems that record everyone entering and leaving the secured area. Door codes shall be changed whenever an employee in possession of the code exits the department or employment with the College.

Visitor Check-In

A Technology Services or Security employee must escort the visitor into the secured area. For long term sessions an IT employee must be readily available in the general area. Clipboards have been installed in all data centers and switch rooms. Visitors must sign in with their name, date, time in and out, and company name.

Recorded: November 4, 2011

Revised: January 27, 2012

Return to Table of Contents