


Name of Policy: Data center / data closet access Policy Number: 3364-65-10 Approving Officer: President Responsible Agent: Vice President of Information Technology Scope: All University of Toledo Campuses	 Original effective date: January 29, 2009
---	--

	New policy proposal	X	Minor/technical revision of existing policy
	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy statement

Unaccompanied access to information technology facilities including all computer rooms, network data closets, and telecommunication closets is restricted to authorized personnel.

(B) Purpose

This policy establishes procedures to secure computer rooms, network data closets, and telecommunication closets from equipment/data theft, vandalism, loss, and unauthorized access.

(C) Scope of policy

The scope of this policy includes university employees, contractors, temporary personnel and other agents of the university who require access to secured information technology facilities.

(D) Procedures

(1) Access requests

- (a) Access to data center facilities in the university computer center, Dowling hall data center, or Ruppert health center computer rooms by non-university personnel (vendor technicians, contractors, etc.) must be requested in advance by calling the information technology help desk. Help desk personnel will then submit a ticket to the data center operations team at which point access will be coordinated with the requester.
- (b) Proper identification is required. Acceptable identification includes a current employer issued identity card or valid driver's license.

- (c) Access shall be granted for, and limited to, work related tasks. The person(s) granted this temporary access shall be escorted and observed at all times by authorized university personnel unless specifically authorized for unescorted access by the director of network services or the manager of data center operations.
- (d) Access for other than work related tasks may be authorized at the discretion of the director of network services or the manager of data center operations. The person(s) granted access for other than work related tasks shall be escorted and observed at all times by authorized university personnel.

(2) Data center / computer room card access

- (a) Card access for data centers and computer rooms is the only unaccompanied mode of entry.
- (b) Temporary card access to data centers and computer rooms will only be granted with approval from the director of network services or the manager of data center operations.
- (c) The director of network services or the manager of data center operations will be responsible for granting permanent access to centers and computer rooms and sending notification to the appropriate staff.

(3) Network data and telecommunications closet access

- (a) Temporary access to network data and telecommunication closets will only be granted with approval from the director of network services or his/her designee.
- (b) The director of network services or his/her designee will be responsible for granting permanent access to network data and telecommunication closets and sending notification to the appropriate staff.

(E) Violations

Violation of this policy will result in appropriate disciplinary action up to and including termination.

Approved by:	Policies Superseded by This Policy: • 004 Computer Room Wiring Closet Security
--------------	--

<p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 29, 2009</u> Date</p> <p><i>Review/Revision Completed by: Vice President of Information Technology</i></p>	<p><i>(former Health Science Campus policy last reviewed 05/05)</i></p> <ul style="list-style-type: none">• Initial Effective Date: January 29, 2009• Review/Revision Date:• Next review date: January 29, 2012
--	--