


<p>Name of Policy: Access control policy.</p> <p>Policy Number: 3364-65-02</p> <p>Approving Officer: President</p> <p>Responsible Agent: Information Security Officer</p> <p>Scope: All campuses – all institutional members</p>	 <p>Effective date: October 11, 2007</p>
<p>X <input type="checkbox"/> New policy proposal</p> <p><input type="checkbox"/> Major revision of existing policy</p>	<p><input type="checkbox"/> Minor/technical revision of existing policy</p> <p><input type="checkbox"/> Reaffirmation of existing policy</p>

(A) Purpose of policy

To provide specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access institutional information assets.

(B) Policy statement

- (1) Each user will be granted a unique user identification and password on the university network.
- (2) User passwords will be kept private at all times.
 - (a) User identification must not be shared or used by anyone other than the user to whom they are assigned;
 - (b) To ensure accurate auditing of user access and actions, user communities, working groups, and departments will not share individual user identifications for system access;
 - (c) Visual representation of passwords in any viewable format in the work area is prohibited;
 - (d) Passwords must be changed for user identification when possible compromise has been suspected or detected;
 - (e) Passwords will adhere to an expiration schedule and require change when expiration occurs.
- (3) Users must only be authorized the minimum level of access to information assets that is required to fulfill an approved institutional need or perform an approved job responsibility.
 - (a) Users must not attempt to gain access to university information systems for which they have not been given proper authorization;

- (b) Users will not grant additional or elevated access to university information systems without proper authorizations or following proper request channels;
- (c) All institutional members who do not belong in an active capacity of the University will have their access suspended or terminated.

(C) Procedure

(1) Delegation of responsibilities

(a) Information technology security and compliance is responsible for:

- (i) Analyzing requests prior to implementation or when circumstances require review.
 - (a) All non-standard requests must be processed by information technology security and compliance.
- (ii) Approving, denying, or revoking access permissions as necessary.

(b) Management is responsible for:

- (i) Ensuring this policy is properly communicated and understood within their respective organizational units;
- (ii) Ensuring all requests for access are submitted by designee of choice;
- (iii) Ensuring the confidentiality, integrity and availability of information assets;
- (iv) Ensuring users in their organizational unit do not have elevated access to systems or access levels which are not required for their job function;
- (v) Ensuring the revocation of access for those who no longer have an institutional need for the information and communicating to human resources prior to the change in accordance with human resources procedures, such as department transfers, leave of absence, termination, etc.

(c) Administrators are responsible for:

- (i) Providing a secure processing environment that protects the confidentiality, integrity and availability of information;
- (ii) Administering access to information as authorized by management;
- (iii) Implementing safeguards;
- (iv) Implementing cost-effective controls;

- (v) Reporting of security concerns or issues to information technology security and compliance;
- (vi) Requesting approval from information technology security and compliance, when the following conditions are requested, but prior to creation:
 - (a) Generic or shared user accounts;
 - (b) Elevated rights to university directory resources;
 - (c) Access originating from external entities of the university;
 - (d) Account creation does not occur through authorized university processes.
- (d) Users are responsible for:
 - (i) Using the information only for its intended purposes;
 - (ii) Maintaining the confidentiality, integrity and availability of information accessed consistent with administrators' approved safeguards;
 - (iii) Maintaining assigned identification codes and/or passwords for purposes of accessing computers, communication links, and information assets.

(2) Enforcement

The failure of any institutional member to perform any obligation required of this policy or applicable local, state and federal laws or regulations will be subject to established university disciplinary actions.

(3) Exceptions

- (a) Requests for exceptions to this policy must be submitted to information technology security and compliance.
 - (i) Each request for exception will be handled on a case-by-case basis;
 - (ii) Each exception approval will be documented by information technology security and compliance.

(4) Definitions

- (a) Authentication: Act of proving an identity's authenticity or validity.
- (b) Authorization: Act of validating the resources an identity is permitted to access.

- (c) Administrators: Are designated by management and/or information technology to manage, process, or store information assets.
- (d) Availability: Assurance that information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is requested.
- (e) Confidentiality: Assurance that information is accessible only to those authorized to have access.
- (f) Identification: Unique credential that identifies somebody or something.
- (g) Information assets: Systems or repositories containing sensitive information or proprietary information.
- (h) Institutional members: Anyone who participates in university activities, or has an affiliation with The University of Toledo. Includes, but is not limited to general staff, managers, medical staff, contractors, vendors, students, alumni and others involved in treatment, payment, or other normal operations of the university, whether or not they are paid by the university.
- (i) Integrity: Assurance that information has not been modified or destroyed in an unauthorized manner.
- (j) Management: Includes senior management, department chairpersons, directors and managers with responsibility for any employees. When management is not clearly implied by institutional design, the chief information office will make the designation.
- (k) Users: Are the individuals, groups, or institutions authorized to access information assets.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 10, 2008</u> Date</p> <p><i>Review/Revision completed by: Vice President, Administration; HIPAA Leadership Committee; JCAHO IM Chapter Committee; IT Leadership; IT Administration</i></p>	<p>Policies superseded by this policy:</p> <p>(none)</p> <p>Initial Effective Date: 10/11/2007 Review/Revision Date: Next Review Date: 10/11/2010</p>
--	---