Name of Policy: **Access control policy.**  

Policy Number: 3364-65-02  

**Approving Officer:** Executive Vice President of Finance and Administration  

**Responsible Agent:** Vice President of Information Technology  

Scope: All campuses – all institutional members  

<table>
<thead>
<tr>
<th>New policy proposal</th>
<th>Minor/technical revision of existing policy</th>
<th>X Major revision of existing policy</th>
<th>Reaffirmation of existing policy</th>
</tr>
</thead>
</table>

Revision date: July 18, 2014  
Original effective date: October 11, 2007

(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. These IDs shall provide the following to the extent possible:

(a) Allow for the identification of an individual that is associated with a given ID;

(b) Take reasonable and appropriate steps so that an individual’s activities can be tracked when accessing EPHI;

(c) The university shall provide a method for creating unique user IDs;

(d) The naming of these IDs shall not convey the privilege level of individual to whom it is assigned.

(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) Users shall immediately report any suspected misuse of their ID or password to the Information Security Office (ISO) or their immediate supervisor;

(f) 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.

(4) All systems shall implement an automatic logoff or locking for users’ sessions.

(a) All users are required to logoff or lock their systems when they are finished with their current session or are expected to be away from their workstation or other EPHI system for an extended amount of time (e.g., lunch, meetings, end of shift);

(b) When feasible, sessions shall be automatically locked or logged off after a specified amount of time as determined by the ISO. Re-authentication shall then be required for a user to regain access to the system;

(c) The ISO shall determine when an automatic logoff/lock is not feasible, and shall approve an alternate locking method (e.g., screensaver locking).

(5) Mechanisms shall be defined for producing reports for auditable events in systems containing PHI, including

(a) Defining frequency of log review.
(b) Identifying person(s) responsible for reviewing log(s)
(c) Processes for reporting identified action items
(d) Retention period for logs and reports

(C) Scope

The scope of this information technology policy includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.
(D) 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 that access requests for users in their organizational unit are limited to systems and access levels required for the user's 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) Data custodians are responsible for:

(i) Approving the content of security classes or reports;

(ii) Approving the proper access to a user in order to enable that user to perform their job function;

(iii) Reviewing their specific areas on a regular basis to validate that access already granted to a user is still appropriate. Formal validation is to be accomplished semi-annually and provided to the administrator for record keeping.

(d) 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) Ensure Banner ERP data custodian validation reports are submitted semi-annually and review reports for necessary corrections.

(vi) Reporting of security concerns or issues to information technology security and compliance;

(vii) 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) 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) Data custodian: Are designated by management (data owners) to authorize users who may have access to particular information in a system or to reports for a specific area.

(g) EPHI: Electronic Protected Health Information

(h) Identification: Unique credential that identifies somebody or something.

(i) Information assets: Systems or repositories containing sensitive information or proprietary information.

(j) 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.

(k) Integrity: Assurance that information has not been modified or destroyed in an unauthorized manner.

(l) 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.

(m) Users: Are the individuals, groups, or institutions authorized to access information assets.
<table>
<thead>
<tr>
<th>Approved by:</th>
</tr>
</thead>
</table>
| David R. Morlock  
Executive Vice President of Finance and Administration  
7/23/14 |

<table>
<thead>
<tr>
<th>Policies superseded by this policy:</th>
</tr>
</thead>
</table>
| Previous 3364-65-02, effective date  
June 24, 2011 |

Initial Effective Date: 10/11/2007  
Review/Revision Date: June 24, 2011; July 18, 2014  
Next Review Date: July 18, 2017

Review/Revision completed by: Vice President, Information Technology; HIPAA Leadership Committee; JCAHO IM Chapter Committee; IT Leadership; IT Administration