3359-11-10.3 Information technology security and system integrity policy.

(A) Need for security and integrity.

The university abides by and honors its long history of supporting the diverse academic values and perspectives engendered in its academic culture, and the university deeply respects the freedom of expression and thought of its users. Although the university does not censor its users' work, exceptional situations may arise where it becomes necessary to protect the integrity and security of university information systems and to provide for effective operation of these systems. The university must, therefore, reserve the right to limit use and access to certain of its computing systems where the university becomes aware of serious violations with respect to its rules and policies, or with respect to applicable federal, state, or local laws and regulations.

This rule provides for information technology system security and integrity. For purposes of this rule, information technology includes computing networks at the university of Akron, which enable communication amongst computing devices as provided by or supported by the university. The security and integrity of information technology shall be protected through a set of priorities with which the university seeks to:

(1) Protect human life and people's safety.

(2) Protect information systems and prevent the unauthorized exploitation of classified or sensitive data, systems, networks or sites.

(3) Protect information systems and prevent the unauthorized exploitation of other data, including proprietary, scientific, managerial and research data.

(4) Prevent any damage to or alteration of information technology hardware or software.

(5) Minimize any disruption of computing resources and processes.

(B) Information technology security officer.

The Chief Information Officer (CIO) shall appoint an information technology security officer ("ITSO") to implement the information technology security program at the university of Akron. The "ITSO" shall seek to assure that information technology is secure at the university and shall be responsible for the following duties:

(1) Providing for network security by seeking to preclude misuse of the university's network to gain or attempt to gain unauthorized access to any system;

(2) Providing for and implementing, in cooperation with the information technology security policy committee, a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate university, law enforcement, or investigative official;

(3) Enforcing the provisions of this rule;

(4) Keeping a record of system integrity problems and incidences;

(5) Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized;

(6) Performing periodic security surveys;

(7) Performing checks of network systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment;

(8) Disposing of software or equipment, through appropriate methods, that university officials deem to be legal or proper where such equipment is not attached to or accessing university network systems;

(9) Ensuring processes are in place to remove all data before equipment is disposed or redeployed;

(10) Training personnel who work with university network systems;

(11) Keeping copies of all records and reports necessary to implement this rule;

(12) Coordinating and consulting with the office of general counsel, the office of the VPCIO and the information technology security policy committee;

(13) Implementing decisions of the university concerning security; and

(14) Providing reports directly to the CIO and the respective vice president in any area where any security violation or potential challenge to security occurs.

(C) Information technology security policy committee.

(1) The CIO shall appoint an information technology security policy committee ("ITSPC") consisting of at least one member from each of the divisions represented by a vice president at the university.

(2) The "ITSPC" shall, in coordination with the "ITSO," recommend written policies and procedures necessary for assuring the security and integrity of information technology at the university of Akron. Additionally, the "ITSPC" shall coordinate

with the "ITSO" in creating and implementing a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity.

(3) Review actions taken by the "ITSO."

(4) The "ITSO" shall be a permanent member of the "ITSPC."

(D) Compliance with system security and integrity; noncompliance and enforcement; reservation of authority and rights.

(1) All university personnel shall cooperate fully with the university "ITSO" and the "ITSPC."

(2) The university reserves the right to take all necessary actions to prevent its network and computing infrastructure from being used to attack, damage, harm or improperly exploit any internal or external systems or networks.

(3) The university reserves the right to take all necessary actions to protect the integrity of its network, the systems attached to it, and the data contained therein.

(4) Violations of federal, state, or university regulations, or any laws respecting information technology will be considered serious matters that may warrant loss of applicable privileges, fines, or more serious action as necessary, including but not limited to appropriate disciplinary action.

(E) Network security and implementation guidelines.

(1) Use of the university's network to gain or attempt to gain unauthorized access to any system or information is prohibited.

(2) Unauthorized network devices may not be attached to the university's network.

(a) An unauthorized network device is any device which, when attached to a packet switched network, enables or facilitates the flow of data for which the device is neither the authorized originator or authorized destination.

(b) Interference with network devices or their functionality is prohibited.

(3) Devices that provide routing service or functionality, or that generate any type of routing protocol traffic, may not be attached to the university's network without justification and the director of network and communications services' prior approval.

(4) Users may not modify the topology of the university's network without prior approval.

(a) The installation of network cables, access points, switches, routers or other

communications equipment by department staff and students is prohibited, without the prior approval of the director of network and communication services.

(b) Telecommunications is the only authorized manager of cable installation.

(5) Network servers.

(a) All network servers and server services must be registered with the server systems group.

(b) The server systems group in the ITS Division will have administrative access to all servers connected to the network to maintain operating system patches and anti-virus software required to protect the university.

(c) Unless arrangements have been made with the server systems group, all network connections are considered to be client connections. Client connections are connections that offer no services, computing resources or data resources to the public internet.

(6) Network applications and protocols that are not essential to carrying out the mission of the university or to the conduct of university business are neither specifically permitted nor specifically prohibited. Should such an ancillary application or protocol become a risk to the security of the university's computing infrastructure, its use may be restricted or blocked as deemed appropriate or necessary, without prior notice.

(7) The use of anonymous or generic "IDs" to provide general login access to university network services is prohibited. This prohibition may not apply when access is otherwise strictly controlled and limited to specific services.

(8) Attempts to bypass or circumvent the university's policies on network security or their implementation are prohibited.

(9) By connecting to the university's network, users consent to the university's use of both active and passive systems to assess the security of the university's network and all devices connected to it.

(a) Systems that appear to be compromised or that present an immediate risk to the security of the university's computing infrastructure may be disconnected as deemed necessary without prior notice.

(b) Those systems not deemed to be high risk will be given ample time to correct the problems.

(10) The university of Akron will make a good faith effort to protect the integrity of all data which traverses its network but does not guarantee its privacy.

Effective:	06/27/2016
Certification:	_____ Ted A. Mallo Secretary Board of Trustees
Promulgated Under:	111.15
Statutory Authority:	3359.01
Rule Amplifies:	3359.01
Prior Effective Dates:	06/09/03, 06/25/07, 01/31/15