3359-11-10 Access and acceptable use of university computer and informational resources.

(A) Authority.

(1) The university of Akron is the legal owner or operator of all university "IT" systems, university "IT" resources and university information stored on those systems and resources.

(B) Definitions and functions.

(1) "IT". "IT" means information technology.

(2) "Systems Authority." "Systems Authority" is the head of a specific subdivision, department, or office of the university who is responsible for oversight of particular "IT" systems, as delegated through the applicable organizational structure. This authority may be delegated through the applicable organizational structure.

(3) "Systems Administrator." "Systems Authorities" may designate another person or persons for purposes of system administration as "System Administrator" to manage the particular system assigned to him or her. "Systems Administrators" oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

(4) "Certifying Authority." College deans, in the case of colleges, and the appropriate vice president, in the case of university administrative units, have "certifying authority" within their area of responsibility, and are thus responsible for certifying the appropriateness and accuracy of an official university document for electronic publication in the course of university business.

(5) "Information Owner." "Information Owners" are those individuals in a specific subdivision, department, or office of the university who have custody of the record information and who are accountable for its use and misuse. These individuals are often referred to as record custodians. "Information Owners" are authorized to determine who is permitted access to particular "IT" resources.

(6) "IT" systems. "IT" systems are the electronic information processing, storage, and transmission systems, which include but are not limited to, the computers, terminals, printers, peripherals, PDAs and other portable devices,

networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the university of Akron. "IT" systems also include, but are not limited to, institutional and departmental information systems, faculty research systems, desktop computers, the university's campus network, and university general access computer clusters.

(7) "IT" resources. "IT" resources are the electronic facilities and electronic access codes and accounts made available to university faculty, staff, contract professionals, students and approved guests, and include but are not limited to computers, networks, telephones, and information.

(8) Specific authorization. Specific authorization is documented permission provided by the applicable "Systems Administrator," "Information Owner," or "Certifying Authority."

(C) Scope. The access and acceptable use policies and related policies from this chapter apply to all "IT" users at the university of Akron and to all "IT" systems and "IT" resources at the university of Akron.

(D) Privileges and responsibilities.

(1) The university of Akron provides "IT" resources and "IT" systems to the university community primarily to serve the interests of the University and its students in the course of normal operations. The provision of such services is in keeping with its academic, instructional, research, administrative and public purpose. Access and usage that do not support the university purpose are subject to restriction and regulation to avoid interference with university work and other applicable directives. All users are obligated to abide by university directives, policies and regulations regarding usage.

(2) Use of and access to "IT" systems and "IT" resources is a privilege, not a right. Except as indicated below, the university does not seek to monitor the communications amongst its many and varied users. The university serves to transmit communications on its "IT" systems and "IT" resources from the senders to intended recipients. Users should not expect any right of privacy in the use of university "IT" systems or "IT" resources since the university may be compelled under public records law, subpoena, investigation, or other law to release information transmitted through the university "IT" systems and "IT" resources. Additionally, the university reserves the right to monitor, review, and release any such communications as necessary for purposes of security, public safety, or other situations such as suspected

disruption to "IT" systems or other shared resources or suspected violations of university rules or procedures or local, state, or federal law. Accordingly, the university reserves the right to make rules and procedures that govern users' access and use.

(3) The University is covered by several federal and state laws and regulations regarding information privacy and security and is committed to protecting the confidentiality, integrity, and availability of all such sensitive and confidential information, including, but not limited to, protected health information and customer information. Therefore, effective "IT" security is the responsibility of every University "IT" user, and every "IT" user is responsible for knowing the rules related to access and acceptable use, privacy, and security.

(E) Acceptable access and use standards.

(1) Users are expected to use "IT" resources and "IT" systems in a responsible and efficient manner consistent with the instructional, research, and administrative goals of the university of Akron. The particular purposes of any "IT" system or "IT" resource, as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.

(2) Use of university "IT" resources and "IT" systems must comply with Ohio law and university policies and directives.

(3) Users are entitled to access only those elements of "IT" systems that are consistent with their specific authorization. Consistent with the organizational structure, "System Authorities," "System Administrators," and "Information Owners" will authorize access to specific systems based on the individual's need to know, the individual's unit, the type of data involved, and the intended use of the information.

(F) Misuse.

(1) Privileges of usage may be denied or removed for the following:

(a) Use that is harassing or threatening to others, or use that violates others' privacy.

(b) Potentially destructive or damaging acts to the integrity of the university of Akron's or other "IT" systems, including, but not limited to:

(i) Attempts to defeat system security.

(ii) Knowing distribution of malware (software designed to infiltrate or damage a computer system without the owner's informed consent) or malicious code.

(iii) Causing disruption, congestion, or security breaches of network communications.

(iv) Engaging in port scanning or security scanning.

(v) Executing any form of "IT" system or "IT" resource monitoring that will intercept data not intended for the user's authorized use, unless this activity is part of the user's normal job or duty at the university.

(vi) Modification or removal of data or equipment.

(vii) Use of unauthorized devices.

(viii) Making "IT" systems or resources available to unauthorized users.

(ix) Unauthorized copying of confidential or sensitive data without the permission of the information technology security officer.

(x) Revealing account password or other authentication methods to others or allowing use of university accounts by others, including family members.

(xi) Circumventing user authentication or security of any "IT" system or resource.

(xii) Use in violation of law.

(c) Use in violation of university contracts.

(d) Disruption or performing unauthorized monitoring of electronic communications.

(e) Unauthorized access or use, which may include, but is not limited to:

(i) Improper access and use of information beyond the individual's authority;

(ii) Attempts to defeat system security;

(iii) Disguised use; or

(iv) Unauthorized sharing of passwords.

(f) Misuse of e-mail, such as, but not limited to:

(i) Sending unsolicited e-mails to a large number of recipients, i.e. sending spam-mail or unwanted chain letters.

(ii) Soliciting for personal financial gain.

(g) Committing crimes or prohibited acts, including but not limited to the following. [Note: Illegal acts involving the university of Akron informational resources facilities may also be subject to prosecution by state and federal authorities].

(i) Use of "IT" systems or "IT" resources for purposes unrelated to the mission of the university.

(ii) Violating the rights of any person or company protected by copyrights or other intellectual property, or software license agreements, which shall include, but not be limited to installation, distribution or copying of technology products/services or copyrighted material for which the user does not have a license.

(iii) Exporting software or technical information in violation of international or regional export control laws.

(iv) Academic dishonesty, including, but not limited to, plagiarism and scientific misconduct, as provided in university rule 3359-11-17.

(h) Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.

(i) Use that is inconsistent with or that jeopardizes the university of Akron’s non-profit status, use for personal gain, use for personal financial gain, and use for promotion of business enterprises.

(G) Procedures for implementing penalties, appeal of administrative decision.

(1) Individuals given the privilege to use "IT" systems and "IT" resources are expected to abide by this and other applicable university of Akron policies, regulations, directives and guidelines. Disregard of this and other applicable policies, regulations, directives and guidelines subjects the user to applicable disciplinary procedures.

(2) Procedures for review of improper access and use.

(a) Procedure for revocation of privileges:

(i) The vice president and chief information officer shall designate a representative who shall collaborate with others as appropriate to review and receive complaints about violations of this policy, and other applicable policies governing computer and informational resources. This designated representative shall have authority to take actions concerning violations of access and use standards, which include, but are not limited to:

(a) Warn users of violations (transmitted electronically or in writing to the user).

(b) Temporarily deny access or suspend usage, based on seriousness of the violation or recurrent violations of other prohibited access and use standards.

(c) Deny access or suspend privileges for a definite time.

(d) Terminate access and privileges for an indefinite time.

(e) Deny access to non-members of the university community whose actions affect or pose a threat to the university.

(ii) To the extent reasonably practicable, warnings will be used to instruct users who may be prone to mistakes, especially while learning new software. Privilege suspension shall only be used for serious or repeated violations of pertinent university rules, regulations, and directives.

(iii) The university at all times reserves the right to take any immediate action necessary to protect the integrity of university "IT" systems and "IT" resources, with or without notice.

(b) Appeal of an administrative decision:

(i) Appeal of a decision made by the designated representative shall be made to the vice president and chief information officer. Thereafter, further appeal may be made to the senior vice president and provost and chief operating officer.

(3) Violations beyond misuse of "IT" systems and "IT" resources will be referred to and addressed by the appropriate office.

Replaces:	3359-11-10
Effective:	01/31/2015
Certification:	_____ Ted A. Mallo Secretary Board of Trustees
Promulgated Under:	111.15
Statutory Authority:	3359
Rule Amplifies:	3359
Prior Effective Dates:	01/13/97, 11/06/06