ASHLAND UNIVERSITY

Policy Name:	**Acceptable Use Policy**					
Section #:	**01**	**Section Title:**	**Information Technology**		**Reviewed:**	**07/27/2017**
Approval Authority:	**ELT**		**Adopted:**	**07/27/2017**	**Next Review:**	**07/01/21**
Responsible Executive:	**Director of I&S**		**Revised:**	**Every 3 years**		
Responsible Office:	**Information Technology**		**Contact:**	**bschwar2@ashland.edu**		
Public Posting or Internal:	**INTERNAL (Portal)**		**Intended Audience:**	**INTERNAL**		

1. Policy Statement

A trusted and effective information technology environment ("IT environment") is vital to the mission of Ashland University. The university provides an IT environment of an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, "AU IT resources" or "resources"). These resources are intended to support AU's teaching, research, and service missions. Access to and usage of AU IT resources entails certain expectations and responsibilities for both users and managers of the IT environment.

2. Reason for Policy

The purpose of this policy is to outline the expectations regarding the acceptable use of IT resources and IT environment by authorized users and to establish the parameters of use.

3. Who Should Read This Policy

All users who have network accounts or by those that have access to IT resources and the IT environment.

4. Resources

5. Definitions

IT Environment - In an information technology (IT) context refers to an enterprise's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services.

IT Resources - All the equipment, networks, hardware, software, technical knowledge, expertise and other resources, including all information technology resources and computer systems, held, owned or used by or on behalf of the institution.

Users - A person who utilizes a computer or network service. A user often has a user account and is identified to the system by a username (or user name).

6. The Policy

1.1. This Policy applies to all individuals using AU IT resources ("Users"), regardless of affiliation and irrespective of whether these resources are accessed from AU's campus or from remote locations. **You are responsible for compliance with all laws and policies.**

1.2. Within AU's IT environment, additional rules may apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to local workplaces, or to specific types of activities (collectively, "local rules"). Local rules must be consistent with this Policy, but also may impose additional or more specific requirements or responsibilities on Users.

1.3. Users will be notified of, or given ready access to (e.g., on a website, portal), this Policy and local rules that govern use of AU IT resources.

1.4. All standards of behavior, courtesy, and etiquette that govern oral and written communications extend into electronic communications.

1.5. The principles of academic freedom apply to electronic communications.

7. Purposes & Appropriate Uses

2.1. AU IT resources are provided for university-related purposes, including support for the university's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

2.2. Users are granted access to AU IT resources for the purposes described in this Policy. Use

should be limited to those purposes, subject to Section 2.3.

2.3. Incidental Personal Use

2.3.1. Users may make incidental personal use of AU IT resources, provided that such use is subject to and consistent with this Policy, including Article 3 of this Policy. In addition, incidental personal use of AU IT resources by an AU employee may not interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment. Incidental personal use that inaccurately creates the appearance that the university is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

2.3.2. Users who make incidental personal use of AU IT resources do so at their own risk. The university cannot guarantee the security or continued operation of any AU IT resource.

2.3.3. Faculty, instructors, and staff may not use AU computing resources and services for commercial and political purposes.

8. User Responsibilities

3.1. Users are responsible for informing themselves of any university policies, regulations, or other documents that govern the use of AU IT resources prior to initiating the use of AU IT resources.

3.2. Use of Resources Accessed through AU IT Resources

3.2.1. When using AU IT resources or resources owned by third parties that are accessed using AU IT resources, Users must comply with all applicable federal and state laws, all applicable university rules, ordinances, and policies, and the terms of any contract or license which governs the use of the third-party resource and by which the User or the university is bound.

3.2.2. In amplification and not in limitation of the foregoing, Users must not utilize AU IT resources to violate copyright, patent, trademark, or other intellectual property rights.

3.2.3. Users will not alternate mobile or computer Operating System without CITO or designated representative prior approval.

3.2.4. Users will not alter or turn-off UserID and Password log-in setup by IT.

3.3. Users may not engage in unauthorized use of AU IT resources, regardless of whether the resource used is securely protected against unauthorized use.

3.3.1. Users must strictly comply with all restrictions relating to the use of AU Confidential Data, (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII), or export-controlled data.

3.3.2. Any records created in the process of doing official AU business are subject to public record laws.

3.3.3. Users must comply with all requirements regarding retention, disclosure, and management of AU data, and return, upon request, any AU data that you place in a cloud service or other external repository.

3.3.4. You must not access AU computers/devices or files belonging to others without proper authorization, and you must not harm AU computers.

3.3.5. Users should report any inappropriate use of data or violation of policy immediately upon discovery.

3.4. Privacy of Other Users

3.4.1. You must not use AU IT resources to violate the privacy rights of anyone.

3.4.1.1. Users are expected to respect the privacy of other Users, even if the devices and systems by which other Users access AU's IT resources, the content other Users place on AU IT resources, or the identities and privileges (rights to access and use certain systems and/or data), of other Users are not securely protected.

3.4.2. Unauthorized use by a User of another User's personal identity or access (login) credentials is prohibited.

3.4.2.1. Users must not share their personal AU NetID password with anyone.

3.4.2.2. Users must not use someone else's AU NetID.

3.5. AU IT resources have a finite capacity. Users should limit their use of AU IT resources accordingly and must abide by any limits AU places on the use of its IT resources or on the use of any specific IT resource. In particular, no User may use any IT resource in a manner which interferes unreasonably with the activities of the university or of other Users.

3.6. AU IT resources may not be used to fundraise, advertise, or solicit unless that use is approved in advance by the university.

3.7. Political Activities

3.7.1. AU IT resources may not be used to engage in political activities on behalf of, or in opposition to, a candidate for public office.

3.7.2. AU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that does not affect the university's interests. AU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that affects the university's interests unless that use is approved in advance by the President.

3.7.3. These prohibitions do not apply to private devices that are attached to the university's network, provided that AU IT resources are not used in a way that suggests the university endorses or supports the activity originating on the private device.

3.8. AU IT resources may not be used to operate a business or for commercial purposes unless that use is approved in advance by the university.

3.9. AU IT resources may not be used to support the operations or activities of organizations that are not affiliated with the University unless that use is approved in advance by the university.

3.10. Pornography and Sexually Explicit Content

3.10.1. Unless such use is for a scholarly or medical purpose or pursuant to a formal university investigation, Users may not utilize AU IT resources to store, display, or disseminate pornographic or other sexually explicit content.

3.10.2. Child pornography is illegal. The use of AU IT resources to store, display, or disseminate child pornography is absolutely prohibited. Any such use must be reported immediately to the Ashland Police Department.

3.11. In operating its IT environment, the university expects Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on their personal devices.

9. Enforcement

4.1. Use of AU IT resources is a privilege and not a right. A User's access to AU IT resources may be limited, suspended, or terminated if that User violates this Policy. Alleged violations of this Policy will be addressed by the CITO or his/her designee.

4.2. Users who violate this Policy, other university policies, or external laws may also be subject to disciplinary action and/or other penalties. Disciplinary action for violation of this Policy is handled through the university's normal student and employee disciplinary procedures.

4.3. In addition to its own administrative review of possible violations of this Policy and other university policies, the university may be obligated to report certain uses of AU IT

resources to law enforcement agencies. (See e.g., Section 3.10.2.)

4.4. If the Chief Information Technology Officer or designee determines that a User has violated this Policy and limits, suspends, or terminates the User's access to any AU IT resource as a result, the User may appeal that decision to the Chief Information Technology Officer (CITO). If the User believes that his/her appeal has not been appropriately addressed by the CITO, he/she may seek further redress as follows:

4.4.1. if an undergraduate student, through the Vice President for Student Affairs, or his/her designee;

4.4.2. if a graduate or professional student, through the Provost, or his/her designee;

4.4.3. if a member of the faculty or academic staff, through the Provost and Director Human Resources, or his/her designee;

4.4.4. if an employee covered by a collective bargaining agreement, through the Director of Human Resources, or his/her designee.

4.5. The CITO or designated representative may temporarily suspend or deny a User's access to AU IT resources when he/she determines that such action is necessary to protect such resources, the university, or other Users from harm. In such cases, the CITO will promptly inform other university administrative offices, as appropriate, of that action.

10. Security & Operations

5.1. The university may, without further notice to Users, take any action it deems necessary to protect the interests of the university and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and blockade of unauthorized access to, and unauthorized uses of, its networks, systems, and data. IT resource administrators may take such actions in regard to the resources they manage without the prior review and approval of the CITO as long as the actions involve automated tools and not direct human inspection.

11. Privacy

6.1. General Provisions

6.1.1. Responsible authorities at all levels of the AU IT environment will perform management tasks in a manner that is respectful of individual privacy and promotes User trust.

6.1.2. Monitoring and Routine System Maintenance

6.1.2.1. While the university does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of those resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities. The university may access IT resources as necessary for system maintenance, including security measures.

6.1.2.2. The university's routine operation of its IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. The creation and analysis of this information may occur at central institutional and local levels.

6.1.2.3. The university may, without further notice, use security tools and network and systems monitoring hardware and software.

6.1.3. The university may be compelled to disclose Users' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Freedom of Information Act (FOIA).

6.1.4. The university reserves the right to monitor and inspect Users' records, accounts, and devices as needed to fulfill its legal obligations and to operate and administer any AU IT resource.

6.1.5. The university may disclose the results of any general or individual monitoring or inspection of any User's record, account, or device to appropriate university authorities and law enforcement agencies. The university may also use these results in its disciplinary proceedings.

6.2. Provisions Regarding Inspections and Disclosure of Personal Information

6.2.1. General provisions:

6.2.1.1. In order to protect User privacy, the Director of Human Resources and CITO or his/her designee must review and approve *any* request for access by a person to an individual User's personal communications or electronically stored information within AU IT resources.

6.2.1.2. Incidental access to the contents of an individual User's personal communications or electronically stored information resulting from system operational requirements described elsewhere in this Policy does not require the prior review and approval of the CITO.

6.2.2. The university, acting through the HR and CITO, may access or permit access to

the contents of communications or electronically stored information:

6.2.2.1. When so required by law. If necessary, to comply with the applicable legal requirement, such disclosures may occur without notice to the User and/or without the User's consent.

6.2.2.2. In connection with an investigation by the university or an external legal authority into any violation of law or of any university policy, rule, or ordinance. When the investigational process requires the preservation of the contents of a User's electronic records to prevent their destruction, HR Director/CITO may authorize such an action.

6.2.2.3. If it determines that access to information in an employee's electronic account or file is essential to the operational effectiveness of a university unit or program and the employee is unavailable or refuses to provide access to the information.

6.2.2.4. If it receives an appropriately prepared and presented written request for access to information from an immediate family member or the lawful representative of a deceased or incapacitated User.

6.2.2.5. If it must use or disclose personally identifiable information about Users without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, or to preserve property from imminent loss or damage, or to prosecute or defend its legal actions and rights.