THE UNIVERSITY of NEW ORLEANS	**Policy No:**	**AP-AA-24.2**
	TITLE:	**Acceptable Use for Information Technology**
	EFFECTIVE DATE:	**July 17, 2014*** **(*Policy Revised, see below)**
	CANCELLATION:	
ADMINISTERED BY: Office of the Vice President for Academic Affairs	**REVIEW DATE:**	**Fall 2017**

PURPOSE

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, research, administration, and service. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles, values, laws, and regulations that govern use of other University facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

AUTHORITY

Part Two, Chapter III, Section IV of the bylaws and rules of the University of Louisiana System.

DEFINITIONS

IT Systems: These are computers, terminals, printers, networks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the University of New Orleans. For example, IT Systems include institutional and departmental information systems, faculty research systems, desktop and laptop computers, the University's campus network, and University general access computer systems.

User: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location. Users include a person who accesses University-owned IT Systems in a University computer cluster, or via an electronic network.

Systems Authority: While UNO is the legal owner or operator of all IT Systems, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("Systems Authority"), or to an individual faculty member, in the case of IT systems purchased with research or other funds for which he or she is personally responsible.

Systems Administrator: Systems Authorities may designate another person as "Systems 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.

Certifying Authority: This is the Systems Administrator or other University authority who certifies the appropriateness of an official University document for electronic publication in the course of University business.

Specific Authorization: This means documented permission provided by the applicable Systems Administrator.

GENERAL POLICY

The policy applies to all Users of UNO Information Technology (IT) Systems, including but not limited to students, faculty, staff, and guests of the University. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by the Office of Information Technology, as well as those administered by individual colleges, departments, University laboratories, and other University-based entities. This includes the general public.

Use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by the University of New Orleans is governed by this Policy.

Respect the rights and sensibilities of others.
Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others is prohibited. Harassing or threatening use is prohibited.

Be aware of the legal implications of your computer use.
Violations of law, and/or university contracts are not permitted.

Respect the mission of the University in the larger community.
Use that is inconsistent with the University's non-profit status is not permitted. Violations of external data network policies are not permitted.

Do not harm the integrity of the University's computer systems and networks.
The individual right to privacy may, when personal files may need to be accessed for troubleshooting purposes, be overridden by authorized personnel to protect the integrity of the University's computer systems.

PROCEDURE

Acceptable use of IT Systems
Although this Policy sets forth the general parameters of acceptable use of IT Systems, faculty, students, and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the University considers acceptable in light of their varying roles within the community. IT Systems Authorities or Administrators may elect to impose stricter controls than those required by this Policy. In all cases where the controls are less restrictive than those of this AUP, this AUP applies.

A. **Acceptable Use**. IT Systems may be used only for their authorized purposes -- that is, to support the research, education, administrative, service, and other functions of the University of New Orleans. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

B. **Proper Authorization**. Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

C. **Prohibited Use**. The following categories of use are unacceptable and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**.
   Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with the University's non-profit status**. The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-UNO purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. Use of IT Systems in a way that suggests **University endorsement of any political candidate or ballot initiative** is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with the President's Office.

4. **Harassing or threatening use**. This category includes, for example, discriminatory harassment, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

5. **Use damaging the integrity of University or other IT Systems**. This category includes, but is not limited to, the following six activities:

   a) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, IT or Systems Administrators from using security scan programs within the scope of their Systems Authority.)

   b) **Unauthorized access or use**. The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-UNO organization or individual may not use non-public IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-UNO organizations or individuals across the UNO network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept

or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

c) **Disguised use**. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

d) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any University-owned or administered equipment or data from IT Systems.

f) **Use of unauthorized devices.** Without specific authorization, Users must not connect networking equipment (routers, hubs, sniffers, etc.) to the Campus network, nor operate network services software (routing, sniffing, name service, multicast services, etc.) on a computer attached to the network, nor physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

6. **Use in violation of law**. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

   With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

7. **Use in violation of University contracts**. All use of IT Systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.

8. **Use in violation of University policy**. Use in violation of other University policies also violates this AUP. Relevant University policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as University, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

9. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

10. **Other inappropriate use.** Accessing material that, in UNO's evaluation, is obscene, defamatory, or constitutes a threat, including pornographic material.

D. **Free Inquiry and Expression**. Users of IT Systems may exercise rights of free inquiry and expression consistent with the principles of the Freedom of Expression Policy adopted by UNO and the limits of the law.

E. **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on any personal or departmental web page.

F. **Encryption of Data**. University faculty and staff, as employees, may encrypt files, documents, and messages for protection against unauthorized disclosure while in storage or in transit. However, such encryption must allow officials, when properly required and authorized, to decrypt the information. A staff member may only encrypt with the permission of his or her supervisor.

G. **Responsibility for Content**. Official University information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

Users also are able to publish information on IT Systems or over UNO's networks. Neither UNO nor individual Systems Administrators can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The University will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual user.

H. **Personal Identification**. Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

Conditions of University Access to Resources

The University places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the University may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant University access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. **Special Conditions**. In accordance with state and federal law, the University may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or

2. When required by federal, state, or local law or administrative rules; or

3. When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

4. When such access to IT Systems is required to carry out essential business functions of the University; or

5. When required to preserve public health and safety.

B. **Process**. Consistent with the privacy interests of Users, University access without the consent of the User will occur only with the approval of the Provost and cognizant Dean (for faculty users), the Provost (for staff users), the College Dean as appropriate (for student users), or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The University, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the Provost, Dean, or other appropriate University authority. A User will be notified of University access to relevant IT Systems without consent, pursuant to A. Special Conditions (1-5) depending on the circumstances, such notification will occur before, during, or after the access, at the University's discretion.

C. **User access deactivations**. In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

D. **Use of security scanning systems**. By attaching privately owned personal computers or other IT resources to the University's network, Users consent to University use of scanning programs for security purposes on those resources while attached to the network.

E. **Logs**. Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of User actions, including the extent of individually-identifiable data collection, data security, and data retention.

F. **Encrypted material**. Encrypted files, documents, and messages may be accessed by the University under the above guidelines. See Acceptable Use of IT Systems (F), above.

User Responsibilities

1. Users shall be issued accounts for the systems to which they are authorized, and the user accounts will remain active for the period the individual is either employed or enrolled, in good standing, at UNO. Retirees and students who graduate from UNO <u>will not</u> be allowed to keep their email account.

   A transition period of 3 months will be provided to each faculty or staff member who ceases their relationship with the university. In order to benefit from the transition period, an individual is required to provide a forwarding email address on or before their final day of employment.

2. Proper use of accounts is the responsibility of the individual to whom it has been assigned. User accounts shall not be shared with others, and all account passwords will be kept secret. Users are expected to change their passwords when there is any suspicion of account theft.

3. Virus protection programs must be installed and updated regularly.

4. The unauthorized use of someone else's account shall be considered theft and computer fraud. Users shall not attempt to gain unauthorized access to any IT system.

5. All communications using university IT systems may be subject to access by the public through public information laws. While some exceptions may prevent a particular email from being sought, these considerations require a case-by-case analysis and users should be aware that confidentiality is not an automatic right in every situation.

Enforcement Procedures

A. **Complaints of Alleged Violations**. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established University Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved who must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

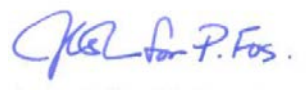
B. **Reporting Observed Violations**. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, who must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

C. **Disciplinary Procedures**. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, the Staff Handbook, the Student Handbook, and other applicable materials. Systems Administrators may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators are authorized to investigate alleged violations.

D. **Penalties**. Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges regardless of fees paid. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. **Legal Liability for Unlawful Use**. In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. **Appeals**. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.



Peter J. Fos, Ph.D., M.P.H.
President
University of New Orleans

**Policy Updates:*
Revisions: 08/05/2015
01/01/2016