Systems and Network Usage Policy

Effective Date: March, 2018

Office: Information Technology

PURPOSE:
The University of Indianapolis maintains a network with finite resources and is primarily intended to support the academic endeavors of our faculty, staff, students, and guests. Any activity that impairs or could impair the confidentiality, availability or integrity of any data, computer system, or network is in direct violation of this policy.

SCOPE:
This policy applies to all members of the University community and guests who have been given permanent or temporary accounts on or access to the University's technology systems, which include all computer systems, networks, UIndy provided devices, data storage, related communication technologies, and information transmitted or maintained on these technologies. This policy also applies whether access is from the physical campus or from remote locations. All members of the University community are responsible for familiarizing themselves with this and any applicable policy prior to use of any campus computing or network resource.

REFERENCE DOCUMENTS/ RELATED INFORMATION: *List any other policies or information that should be cross referenced.*

POLICY HISTORY: *Include any information about previous versions or whether this replaces an existing policy.*

I. Systems and Network Integrity

The University of Indianapolis maintains a network with finite resources and is primarily intended to support the academic endeavors of our faculty, staff, students, and guests. Any activity that impairs or could impair the confidentiality, availability or integrity of any data, computer system, or network is in direct violation of this policy. Penalties for violation could include termination or expulsion.

Such actions include, but are not limited to, the following:

- unauthorized use of systems or accounts
- use of any UIndy account by anyone other than the account owner
- impersonation of other individuals in communications
- attempts to crack or capture passwords
- attempts to break encryption protocols
- compromising privacy
- destruction or alteration of data or programs belonging to other users
- attempts to steal or destroy software
- creation of a trojan, spyware, worm, virus, or other malware
- reverse engineering software or hardware in an attempt to discover or exploit vulnerabilities, disrupt systems or violate copyright
- running programs or processes that disrupt or interfere with the University's operation of its computer systems
- using computer systems for the purposes of abuse, harassment, or stalking
- using technology in any way that violates local, state, or federal laws
- using technology in any way that violates other University policies
- using technology in any way that violates academic integrity, such as cheating, research misconduct (i.e. fabrication, plagiarism, and/or falsification), detrimental research practices (e.g. improper data storage/security) or assisting others in violating academic integrity

In addition, users may not:

- conduct experiments to identify or demonstrate system or network vulnerabilities without prior written permission from Information Technology
- attach network hubs, bridges, routers, or gateways to the campus network
- use University network addresses without permission from UIndy Information Technology
- use excessive amounts of technology resources—such as bandwidth and/or disk storage on University servers

II. Privacy

University of Indianapolis respects every individual’s rights and legitimate expectation to privacy in the electronic forum and prohibits users of University resources, including University- and personally- owned devices linked to the University network, servers and telecommunications equipment from violating such rights. Examples of violations of privacy rights include, but are not limited to, the following:

- unauthorized access to another person’s electronic communications
- unauthorized access to another person’s files

- unauthorized access to another person's electronic records
- using another person's password

Users of University computers and networks should understand that the University makes no claims of privacy, nor should users expect privacy while using any computer connected to the Internet. When using University or personal resources that require privacy, appropriate measures, such as encryption, must be taken to ensure confidentiality and integrity of data.
University employees whose job functions may require accessing private directories, data, or software must make reasonable efforts to respect the privacy of others. Supervisors, for example, must make reasonable attempts to respect an employee's privacy while accessing job-related materials. UIndy's Information Technology staff may need to access data and software stored on University computers while providing maintenance or safeguarding the integrity of systems and networks. Information Technology staff must first make reasonable efforts to maintain system integrity by means which do not involve accessing or collecting sensitive data.

III. Appropriate and Ethical Use

The University of Indianapolis expects its constituents to use information technology in ways that are legal, ethical, and appropriate in support of the University's mission. Actions which are unethical or inappropriate include, but are not limited to, the following:

- sending unsolicited advertising, promotional material or other forms of mass mailing solicitation, except in those areas that are designated for such purpose such as the classified ad area
- using University-owned computers for personal monetary gain or commercial activities inconsistent with University's mission
- displaying in a public setting electronic materials which may be distracting, intimidating, or harassing to others
- using University technology resources to store or transmit electronic information with harassing or intimidating content

IV. Copyright and Licensing

All users of University-owned computers are expected to abide by copyright laws and licensing agreements. No user may copy or attempt to copy, without authorization, any proprietary or licensed software provided or installed by the University. By the terms of the Berne copyright conference (now part of the United States law), virtually all material fixed in a tangible medium, including photos, text (printed and electronic), music, software, and broadcast performance is copyrighted. This is true whether or not copyright was registered and whether or not the material was published prior to the Berne accords.

The "fair use" concept of the 1976 copyright law allows borrowing of small amounts of materials for such uses as "criticism, comment, news reporting, teaching, scholarship, or research" (U.S Code, Title 17, Sect 107). The test of fair use addresses (1) the purpose and character of the use; (2) the nature of the work copied; (3) the amount and substantiality of portion copied; and (4) market effect.

The Director of Technology Planning and Acquisition will provide, upon request, information about software licensing, and the Director of the Library will provide information about copyright.

V. Availability

Information Technology performs maintenance on its systems at published times. Emergency maintenance and outage notifications will be posted as soon as possible to the campus. It is each user's responsibility to remain aware of posted maintenance schedules and plan activities accordingly. Information Technology regularly conducts system-level backups in case of a catastrophic failure, but cannot provide backup files in cases of accidental deletion by the user. It is advisable that every user retains his or her own backup copies of important files he or she maintains.

VI. Reporting Violations

If an employee or student suspects that an individual is engaged in activities violating this policy, the incident may be reported to the IT Help Desk or University Police.

VII. Disciplinary Actions

The University may take disciplinary and/or legal action against any individual who violates these policies. Such actions include, but are not limited to, suspension of an individual's use privileges to the University's computing facilities, expulsion or termination from the University.

VIII. Exceptions

Occasionally, deviations from this policy will be necessary in support of academic pursuits or business processes. Requests for exceptions to this policy should be sent to help@uindy.edu. Information Technology staff will evaluate the request, risk and compensating controls in determining whether to approve of such a request. Exceptions that create significant risk without compensating controls will not be approved.