Policy Library

810 Acceptable Use of Information Technology

Authority: Approved by the Board of Trustees

Last updated on: May 06, 2022

810.1 Purpose

Indiana State University provides a variety of computing resources to its campus and public constituents. Those who use University information resources are to take reasonable and necessary measures to safeguard the operating integrity of institutional systems and data. This policy covers aspects of legitimate use, information security, and privacy that arise in the use of computers, software, and electronic information. This policy strives to balance the individual's ability to benefit fully from these resources and the University's responsibility to maintain the accessibility, integrity, utility, and security of the electronic information environment.

The University's responsibilities in this area can generally be described as the delivery of information technology resources that are stable, reliable, and secure, and the delivery of support for those resources. In the information technology environment today, individuals and the institution play a role in meeting those responsibilities. As context for the requirements of acceptable use by individuals, it is helpful to understand in more detail some of the institutional duties in providing and supporting information technology. These include:

a. Ensuring efficient and reliable performance of University computer systems and networks.

b. Establishing and supporting reasonable standards of security for electronic information that University community members produce, use, or distribute.

c. Protecting University computers, networks and information from destruction, tampering, unauthorized inspection and use.

d. Ensuring that information technology resources are used in a manner consistent with the University's mission.

e. Defining the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing unlawful activities.

f. Ensuring that University computer systems do not lose important information due to hardware, software, or administrative failures or breakdowns.

g. Communicating University policies and individuals' responsibilities systematically and regularly in a variety of formats, to all parts of the University community.

h. Monitoring policies and proposing changes in policy as events or technology warrant.

i. Managing computing resources so that members of the University community benefit equitably from their use.

j. Enforcing policies by restricting access in case of serious violations (see section on "Sanctions").

810.2 Scope

This policy applies to the use of all computing devices owned by Indiana State University, and to all computing devices owned by others that are attached to the institutional network or used in the processing of institutional business or the creation, receipt, transmission, processing, use, storage, printing, or dissemination of institutional data.

810.3 User Responsibilities

Indiana State University supports networked information resources to further its mission and to foster a community of shared inquiry. All members of the University community must be cognizant of the rules and conventions that make these resources secure and efficient. It is the responsibility of each member of the University community to comply with all applicable University Information Technology policies and standards, including the following standard practices.

810.3.1 Respect the Rights of Others. Users are expected to (i) respect the right of others to be free from harassment or intimidation to the same extent that this right is recognized in the use of other communications media and (ii) respect the privacy of other community members, regardless of whether their accounts are securely protected. Consequently, although each user has the right to freedom of speech, unlawful or harassing material may not be sent or displayed to others.

810.3.2 Respect Intellectual Property Rights. Respect copyright and other intellectual property rights. Unauthorized copying of files or passwords belonging to others or to the University may constitute plagiarism or theft. Modifying files without authorization (including altering information, introducing viruses or other malware, or damaging files) is unethical and may be illegal.

810.3.3 Maintain Secure Passwords. Users must establish appropriate passwords in the first instance, and should use different passwords for University accounts than are used for non-University accounts. Passwords must not be shared with others. This means that, except in emergency situations, University employees must not give someone else their password, and they must not accept a request, offer, or direction to use someone else's password. If an emergency situation arises where a user's password must be shared to perform a specific function, that password must be changed immediately. For accounts used in University operations, and for applications or services where University data is stored, users must change their password every six months, at a minimum. If a password is compromised, or if it is suspected or known that another individual has learned a user's password, the user must change their password immediately. Passwords should not be stored or transmitted through electronic communications, but if they must be, they must be encrypted.

810.3.4 Identify Oneself Accurately. Users are expected to identify oneself accurately and appropriately in electronic communications.

810.3.5 Use Resources Efficiently. Users should accept limitations or restrictions on computing resources such as storage space, time limits, or amount of resources consumed when asked to do so by authorized personnel. University resources are to be used in a manner consistent with the University's mission. Use of University resources for personal activities should in no way interfere with or take precedence over institutional uses. Indiana State University computing resources may not be used for commercial purposes.

810.3.6 Recognize Limitations on Privacy. Users should recognize the limitations to privacy afforded by electronic services. Users have a right to expect that what they create, store, and send will be seen only by those to whom permission is given. Users must know, however, that the security of electronic files on shared systems and networks is not inviolable – most people respect the security and privacy protocols, but a determined, technically-well-informed person may be able to breach them. Users must also note that, as part of their responsibilities, systems or technical managers may occasionally need to diagnose or solve problems by examining the contents of system files. Furthermore, when a personal device is

used in the conduct of University business, there should be no expectation of privacy related to University data stored on or transmitted by that personal device.

810.3.7 Recognize University's Maintenance of Network. An individual's right to privacy may be superseded by the University's responsibility to maintain the network's integrity. Should the security of the network or a computer system be threatened, a person's files may be examined by an OIT administrator with approval from the Provost and Vice President for Academic Affairs or Associate Vice President for OIT or General Counsel. By law, instances can arise when material created or received via electronic means must be divulged (i.e., pursuant to a validly issued subpoena in connection with legal action).

810.3.8 Abide by Security Restrictions. Abide by security restrictions on all systems and information to which access is permitted. Users should not attempt to evade, disable, or "crack" passwords or other security provisions.

810.3.9 Comply with All Applicable Local, State and Federal Laws and Regulations and Policies of the University. Users must abide by all applicable local, state and federal laws. Indiana State University extends these principles and guidelines to systems outside the University that are accessed via the University's facilities (i.e., electronic mail or remote logins using the University's Internet connections). Network or computing providers outside Indiana State University may also impose their own conditions of appropriate use for which users at this University are responsible. For violations of the above, see the "Sanctions" section of this policy.

810.3.10 Abide by Export Controls. Indiana State University and its faculty, staff, and students must comply with all United State export control laws and regulations. Export control laws cover assets of the institution when they are taken or shipped to locations outside the United States, and in some cases when foreign nationals have access to certain kinds of equipment within the United States. Faculty, staff, and students are responsible for understanding whether equipment they are working with or responsible for is covered by export regulations in cases where they are traveling outside the United States, or working with foreign nationals inside the United States. Please see the Export Control webpage for more information.

810.3.11 Abide by Security Restrictions and Best Practices When Using Personal Devices for Institutional Business. Users should maintain awareness of, understand, and follow policies and recommended best practices for security when using personal mobile or other devices to access institutional resources such as Internet-based services and electronic mail accounts. When specific standards are identified by the institution, abide by those standards. Personal devices used

to create, access, store, transmit, use, or process institutional data or perform institutional business must adhere to institutional standards for data and information security (see Policy 830 Data Security and Management). In particular, a personal device used for institutional business, including electronic mail, or to store institutional data must be password protected

810.3.12 Protect the University's Information Technology Resources. The University employs numerous measures to protect the security and integrity of its information resources and networks but cannot solely prevent unauthorized access or compromised accounts. Users are responsible for following published security guidance to ensure that all their devices that access ISU's resources are adequately protected. All users with ISU information technology resources must promptly report all information security incidents to the Office of Information Technology using the published incident report procedure available on the OIT website.

810.4 Department and Individual Responsibilities with Servers

810.4.1 Approval Required. Servers that are not maintained by OIT must be registered with and approved by OIT prior to their connection to the institutional network. Unregistered servers that are detected on the network may be disconnected and removed without notice by OIT.

810.4.2. Security. Servers and applications that are run on those servers that are not supported by OIT must be maintained at all times to a current level of upgrade for security. OIT may audit such servers at any time.

810.5 Sanctions

Individuals or groups who act in a manner contrary to existing policy and accepted standards for computer use or who take actions which have legal implications are subject to appropriate sanctions.

810.5.1 Suspension or Revocation of Privileges. Indiana State University reserves the right, at all times, to suspend or revoke the privilege of access to University electronic services. Violations of information technology policies will be dealt with in the same manner as violations of other University policies and may result in disciplinary review.

810.5.2 Role of Office of Information Technology. As a first step, such matters will be addressed by the appropriate Office of Information Technology (OIT) administrator. Whenever it becomes necessary to enforce University rules or policies, the University may take the following steps, and any other steps it deems

appropriate to address the use or misuse of University electronic services. An authorized OIT administrator may:

a. Disallow network connections by certain computers (departmental or personal).

b. Require adequate identification of computers and users on the network.

c. Undertake audits of software or information on shared systems where there is sufficient reason to suspect policy violations.

d. Take steps to secure compromised computers that are connected to the network.

e. Restrict or deny access to computers, the network, and institutional software and databases.

f. Refer the matter for disciplinary action.

810.5.3 Cooperation in Investigation. Users are expected to cooperate with authorized investigations either of technical problems or of possible unauthorized or irresponsible use as defined in these guidelines; failure to do so may be additional grounds for suspension or termination of resource access privileges.

810.5.4 Appeal. If a matter is not resolved in discussion with the OIT administrator within 24 hours, the OIT administrator's action may be appealed to the administrator's direct supervisor or referred to the appropriate University administrator for resolution in a timely manner. Any revocation of privileges is subject to the normal due process available to all members of the faculty, staff and student body.

> **810.5.4.1 Civil/Criminal Concerns.** In addition, certain kinds of abuse (such as copyright violation, fraud, violation of software licenses, or harassment) may entail initiation of civil or criminal investigation and/or prosecution.

810.5.5 Additional Questions. Additional questions relating to this policy should be directed to the Chief Information Officer in the Office of Information Technology.