

## 930 INFORMATION TECHNOLOGY RESOURCES POLICY

*Policy 930 was included in the 2001 University Handbook revision.*

**930.1 Overview.** The University is committed to an open flow of information within and between the University and the public. Those who use University information resources are to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others while acting to maintain a working environment conducive to carrying out the University's mission of instruction, research and scholarship, and public service. The following policies introduce issues of legitimate use, information security, and privacy that arise in the use of computers, software, and electronic information. These policies strive 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.

### 930.2 University Responsibilities.

**930.2.1 General University Responsibilities.** The University owns or leases most of the computers and computer networks used on campus and has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility to administer, protect, and maintain its aggregation of computers, software, and networks.

**930.2.2 Specific University Responsibilities.** Specifically, the responsibilities of the University are to:

- a. Ensure efficient and reliable performance of University computer systems and networks.
- b. Establish and support reasonable standards of security for electronic information that University community members produce, use, or distribute.
- c. Protect University computers, networks and information from destruction, tampering, unauthorized inspection and use.
- d. Ensure that information technology resources are used in a manner consistent with the University's mission.
- e. Delineate the limits of privacy that can be expected in the use of networked computer resources and preserve freedom of expression over this medium without countenancing unlawful activities.
- f. Ensure that University computer systems do not lose important information because of hardware, software, administrative failures or breakdowns. To achieve this objective, authorized systems or technical managers may occasionally need to examine the contents of system files to diagnose or solve problems.
- g. Communicate University policies and individuals' responsibilities systematically and

regularly in a variety of formats to all parts of the University community.

h. Monitor policies and propose changes in policy as events or technology warrant.

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

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

**930.3 Individual 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:

**930.3.1 Respect Others.** 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. Consequently, although each user has the right to freedom of speech, unlawful material may not be sent or displayed to others.

**930.3.2 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 Trojan horses, or damaging files) is unethical and may be illegal.

**930.3.3 Maintain Passwords.** Maintain secure passwords. Users should establish appropriate passwords in the first instance, change them occasionally, and not share them with others. This is necessary to maintain privacy and to assure accountability as a consumer of University resources.

**930.3.4 Identify Oneself Accurately.** Identify oneself accurately and appropriately in electronic communications.

**930.3.5 Use Resources Efficiently.** Use resources efficiently. 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. Indiana State University computing resources may not be used for commercial purposes.

**930.3.6 Recognize Limitations on Privacy.** 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.

**930.3.7 Recognize University's Maintenance of Network.** In addition, 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 designee. Finally, 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).

**930.3.8 Archive.** Learn to use software and information files correctly. Users should maintain and archive backup copies of important work. Users are responsible for backing up their own files. If users depend upon OIT backup service, they should become familiar with the schedules and procedures of that service.

**930.3.9 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; these activities threaten the work of others and are grounds for immediate suspension or termination of privileges and possible further sanctions.

**930.3.10 Abide by Laws.** Abide by all applicable federal and state 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.

**930.4 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.

**930.4.1 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.

**930.4.2 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.

**930.4.3 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.

**930.4.4 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.

**930.4.4.14 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.

**930.4.5 Additional Questions.** Additional questions relating to information technology resources policies should be directed to the Executive Director, Office of Information Technology.

*Last revised February 1, 2011.*