ACCEPTABLE USE POLICY

1. Purpose

This policy addresses the use of information technology resources (IT resources) at Indiana University of Pennsylvania ("the university"). IT resources are intended to support the university's instructional, research, and administrative operations.

2. Scope

This policy applies to all users of IT resources owned or operated by Indiana University of Pennsylvania. Users include students, faculty, staff, contractors, and guest users of computer network resources, equipment or connecting resources.

3. Objective

The objective of this policy is to create a framework to ensure that IT resources are used in an appropriate fashion, and support the university's mission and institutional goals.

4. Policy

Use of the university's IT resources is a privilege and signifies agreement to comply with this policy. Users are expected to act responsibly, and follow the university's policies and any applicable laws related to the use of IT resources. This policy provides regulations to assure IT resources are allocated effectively.

While the university recognizes the role of privacy in an institution of higher learning, and will endeavor to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned IT resources, except as required by law. For example, the university may be required to provide information stored in IT resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the University may also be viewed by technical staff working to resolve technical issues.

5. Definitions

Information Technology (IT) resources include, but are not limited to, all university owned or operated hardware, software, computing equipment, systems, networks, programs, personal data assistants, cellular phones, fax, telephone, storage devices, cable television, input/output, connecting devices via either a physical or wireless connection regardless of the ownership of the device connected to the network, and any electronic device issued by the university. IT resources include all electronic media, voice, video conferencing and video networks, electronic mail, and related mediums such as blogs, wikis, websites, and electronic records stored on servers and systems.

6. Responsibilities

A. Responsibilities of Users of IT Resources

1. Respect the intellectual property of authors, contributors, and publishers in all media.
2. Protect user identification, password information, and the system from unauthorized use.
3. Adhere to the terms of software licenses and other contracts. Persons loading software on any university computer must adhere to all licensing requirements for the software. Except where allowed by university site licenses, the copying of university-licensed software for personal use is a violation of this policy.
4. Comply with federal, state, and local laws, relevant university personal conduct regulations, and the terms and conditions of applicable collective bargaining agreements. Applicable laws include, but are not limited to, those regulating copyright infringement, copyright fair use, libel, slander, and harassment.

5. Become acquainted with laws, licensing, contracts, and university policies and regulations applicable to the appropriate use of IT resources. Users are expected to use good judgment and exercise civility at all times when utilizing IT resources, and respect the large, diverse community utilizing these resources in a shared manner.
6. Understand the appropriate use of assigned IT resources, including the computer, network address or port, software, and hardware.
7. Comply with the university's Use of E-mail as an Official Means of Communication Policy. Electronic mail should never be considered an appropriate tool for confidential communication. Messages can be forwarded or printed, and some users permit others to review their e-mail accounts. Message content can be revealed as part of legal proceedings. Finally, messages are sometimes not successfully delivered due to a technical issue requiring authorized IT personnel to review message content as part of the troubleshooting process.

B. Prohibited Uses of IT Resources

1. Providing false or misleading information to obtain or use a university computing account or other IT resources.
2. Unauthorized use of another user's account and attempting to capture or guess passwords of another user.
3. Attempting to gain or gaining unauthorized access to IT resources, or to the files of another user. Attempting to access restricted portions of the network, an operating system, security software or other administrative applications without authorization by the system owner or administrator.
4. Interfering with the normal operation, proper functioning, security mechanisms or integrity of IT resources.
5. Use of IT resources to transmit abusive, threatening, or harassing material or other communications prohibited by law.
6. Copyright infringement, including illegal sharing of video, audio, software or data.
7. Excessive use that overburdens or degrades the performance of IT resources to the exclusion of other users. This includes activities which unfairly deprive other users of access to IT resources or which impose a burden on the university. Users must be considerate when utilizing IT resources. The University reserves the right to set limits on a user through quotas, time limits, and/or other mechanisms.
8. Intentionally or knowingly installing, executing, or providing to another, a program or file, on any of the IT resources that could result in the damage to any file, system, or network. This includes, but is not limited to computer viruses, trojan horses, worms, spyware or other malicious programs or files.

7. Procedures

1. Violations of this policy will be reported to appropriate levels of administrative oversight, depending on the statutes and policies violated. Suspected violations of federal and state statutes and local ordinances shall be reported to the Director of Public Safety (chief of campus police) for official action.
2. Non-statutory violations of the Acceptable Use Policy, such as "excessive use," may be reported to the Chief Information Officer, the Associate Vice President for Human Resources, the Office of Student Conduct and/or the Director of Public Safety (chief of campus police).
3. A university employee or student who violates this policy risks a range of sanctions imposed by relevant university disciplinary processes, including denial of access to any or all IT resources. He or she also risks referral for prosecution under applicable local, state or federal laws.
4. The University Senate – via the Library and Educational Services Committee – is responsible for recommending the university's Acceptable Use Policy. Questions

regarding the applicability, violation of the policy or appropriate access to information should be referred to the Chief Information Officer.

8. Rescission

1. Computing Resources Policy
2. Computer Software Policy
3. E-mail Privacy Policy

9. Publications Statement:

This policy should be published in the following publications:

1. Administrative Manual
2. Student Handbook
3. IUP Catalog
4. IUP Website

10. Distribution

1. All Employees
2. All Students
3. All affiliates with access to IT resources at IUP