Indiana University of Pennsylvania

IT Acceptable Use Policy

Navigate IT Support

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.

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.

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.

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.

Definitions

For the purposes of the IUP Acceptable Use of IT Resources Policy (AUP), IT resources include the university computer network, all university-owned devices, and all university-provided software systems regardless of what computer network is being used. This is inclusive of all content transmitted over the university computer network by any device regardless of ownership.

The National Institute of Standards and Technology (NIST) defines Personally Identifiable Information (PII) as any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Responsibilities

Responsibilities of Users of IT Resources

- Respect the intellectual property of authors, contributors, and publishers in all media.
- Protect user identification, password information, and the system from unauthorized use.
- 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.
- 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.
- 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.
- Understand the appropriate use of assigned IT resources, including the computer, network address or port, software, and hardware.
- 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.
- Protect Personally Identifiable Information (PII) on IUP's network by only storing sensitive information when necessary on university drives, and adhering to best practices for the proper storage of PII.
- Adhere to the Portable Storage Device Procedure

Prohibited Uses of IT Resources

- Providing false or misleading information to obtain or use a university computing account or other IT resources.
- Unauthorized use of another user's account and attempting to capture or guess passwords of another user.
- 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.
- Interfering with the normal operation, proper functioning, security mechanisms, or integrity of IT resources.
- Use of IT resources to transmit abusive, threatening, or harassing material.
- Copyright infringement, including illegal sharing of video, audio, software, or data.
- 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.
- Intentionally or knowingly installing, executing, or providing to another a program or file on any of the IT resources that could result in 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.

Procedures

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.

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 Support and Community Standards, and/or the director of Public Safety (chief of campus police).

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.

The University Senatevia 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.

Portable Storage Device Procedure

This procedure is a specific extension of the IUP Acceptable Use of Information Technology Resources Policy. As such, the Senate Library and Educational Services Committee (LESC) is responsible for recommending changes to the procedure.

IT Services-managed desktops and laptops permit the use of portable electronic storage devices. These devices include flash drives, memory sticks, data disks, etc. The university reserves the right to conduct security scans on portable storage devices connected to the network.

Users are strongly encouraged to store only non-sensitive data on these devices. When sensitive data is stored, IT Services encourages the use of data encryption. Users can submit an ihelp ticket to obtain data encryption assistance.

The university is not responsible for backing up data stored on these devices. As these devices are susceptible to loss, theft, data corruption, or damage, users are strongly encouraged to back up the data to a non-portable storage device. The university is not liable for any data loss on these devices.

Rescission

- Computing Resources Policy
- Computer Software Policy
- Email Privacy Policy

Publications Statement

This policy should be published in the following publications:

- Administrative Manual
- Student Handbook
- IUP Catalog
- IUP website

Distribution

- All employees
- All students
- All affiliates with access to IT resources at IUP

Document History

April 2018 - Added Protect Personally Identifiable Information responsibility per 3/6/2018 Senate approval

April 2017 - Updated language per Senate

April 2014 - Removed ambiguous phrase

IT Support Center

Delaney Hall
950 Grant Street
Indiana, PA 15705

Phone: 724-357-4000

VIRTUAL IT SUPPORT VIA
Zoom

https://iupvideo.zoom.us/my/virtualitsupportcenter
Fall and Spring Semesters:
Monday through Friday:
8:00 a.m.–Noon

it-support-center@iup.edu

1:00 p.m.–4:30 p.m.

Summer and Winter Sessions:

Monday through Friday:

8:00 a.m.–Noon

1:00 p.m.–4:00 p.m.

DELANEY OFFICE HOURS

Fall and Spring Semesters:

8:00 a.m.–4:30 p.m.

Summer and Winter Sessions:

8:00 a.m.–4:00 p.m.