ILLINOIS TECH

Acceptable Use Policy

Version:	2.3
Date of version:	April 10, 2024
Created by:	S Beidas
Approved by:	K Christensen & S Vaishnav
Confidentiality level:	INTERNAL USE

ILLINOIS TECH

Table of Contents

ILLINOIS TECH

Purpose

The purpose of Illinois Tech's Acceptable Use Policy is to outline the requirements for the authorized usage of any Illinois Tech (also referred to herein as the "University") technology and digital resources, including devices, computers, networks, equipment, cyber security, applications, and cloud-based infrastructure.

This policy applies to use occurring (i) while utilizing any University network, (ii) on campus, (iii) at any University-owned building or property, (iv) at any University event on or off campus, and (v) remotely from any location whatsoever.

This policy further applies to all University electronic information accessed by users.

Lack of compliance with this policy or any associated University policies, standards, or plans, may result in sanctions including, without limitation, those outlined below. Failure to complete either University-mandated Cybersecurity Awareness Training or remediation of AUP violations may result in disciplinary action, remedial or corrective measures, and/or sanctions deemed appropriate by Illinois Tech.

Policy Statement

Through the annual acceptance of the Acceptable Use Policy (AUP), Illinois Tech users ~~must~~ agree to abide by the University's policies and rules for using the University's Technology Resources. Use of Illinois Tech's Technology Resources and access to its networks are privileges granted by the University to authorized users and may be suspended with or without notice.

Illinois Tech may, in its sole discretion, terminate access if the University has reason to believe users have violated the University's policies. Violations may include, but are not limited to, the following:

- Improperly using Illinois Tech's Technology Resources
- Interfering with the work of others
- Causing a security risk to Illinois Tech or others
- Degrading the performance or availability of services to others
- Violating federal, state, or local laws, including but not limited to copyright protection

Scope

This policy applies to Illinois Tech Community Members, Friends, and anyone else granted access to any University Technology Resources .

This policy applies at all Illinois Tech locations, including affiliate and offsite locations where users access University resources in person and/or remotely. This policy applies regardless of where users

access University Technology Resources for any use, including academic and instructional uses, class assignments and faculty and student research.

This policy includes sanctions for any Illinois Tech Community Member or Friend, as well as anyone else, who is not in compliance with Illinois Tech security policies.

Sanctions may be imposed due to regulatory, legal, contractual, training, and grant compliance requirements. Please see the Sanctions section for specifics.

Definitions are provided in the Glossary.

Policy

Policy Principles

- **Academic Freedom:** The principles of academic freedom may apply to electronic communications.
- **Legal Requirements:** The use of Technology Resources is subject to the University's policies, plans and standards as well as laws and regulations.
  Required Conduct: Using Illinois Tech's systems and networks is a privilege, not a right. Violations of this policy due to intentional or unintentional acts may result in suspension or termination of access. Users are required to refrain from circumventing, jeopardizing or willfully damaging the University's Technology Resources and connectivity to them. This could also result in notifications to legal authorities in cases of potential transgression of the law.
- **Technology Resources refers to all technologies that produce, manipulate, store, communicate, or disseminate information.** These resources include wired and wireless data, data at rest, video and voice networks, Virtual Private Networks (VPN), computers for processing information, and other devices for storing, transmitting, and archiving information. This includes equipment connected to these networks (regardless of ownership), and equipment owned and/or registered to the University and its affiliates for all University locations.

Acceptable and Authorized Usage

- The Office of Technology Services (OTS) supports Illinois Tech's primary technology systems. The OTS Infrastructure Team maintains Illinois Tech's internal data center, networking and computer equipment rooms, office areas, and cloud facilities. OTS is responsible for managing the integrity of the University's system infrastructure and networks as defined above. This includes monitoring appropriate usage and access.

- Unauthorized usage, transfer of data, security risks, or any other activities that the University believes or determines poses a cybersecurity risk to the University may result in suspension or termination.
- Authorized users are validated in accordance with Illinois Tech's Access Control Plan, Authentication Standard, and Muli-Factor Authentication Standard. Authorized users shall ensure that access, usage, and transfer of data shall be in accordance with the aforementioned policies at all times.
- Illinois Tech's Technology Resources may not be used for illegal or improper use, including commercial purposes for profit-generation or other purposes that conflict with the University's objectives and mission. This includes, but is not limited to, intentionally breaching security, using unauthorized licensed software, deploying malware, or creating programs, web forms, or other mechanisms that authenticate using Illinois Tech credentials.
- Unique identifiers supplied by Illinois Tech to users to access systems and networks remain University property. These identifiers may be revoked at any time for any reason.
- Authorized Illinois Tech users are responsible for maintaining privacy of passwords and maintaining proper identification of their email by properly identifying sender.
- The use of unauthorized credentials for which users are not explicitly granted or an attempt to capture credentials to access unauthorized accounts is prohibited. To either share passwords or enable any unauthorized access to Technology Resources is a direct violation and may result in sanctions.
- Non-Illinois Tech users, such as contractors and program guests, must request "Friends User Role" to obtain access to the University's systems and networks, regardless of ownership of device used to access the University's Technology Resources or location(s). The unit to which the non-Illinois Tech user is associated with is responsible for the submission of these requests for OTS approval.
- The contents of Illinois Tech email accounts are the property of the University. Users should not assume complete confidentiality or privacy when using their Illinois Tech email accounts.

Application Usage

- **Application Use on University-owned assets:** All applications utilized on university-owned devices must be vetted for use by OTS.
- **Cloud-based Integration Requests:** Applications that require access to cloud resources may be denied or revoked for any reason by the University.
- **Mandatory Use of Microsoft 365 Applications and Google Plug-Ins:** Illinois Tech users are required to utilize only official plug-ins authored and published by Microsoft 365 and Google when utilizing Microsoft 365 and Google applications. Third-party applications that connect to either Microsoft 365 or Google Apps are not allowed without prior approval.

Note: The use of Microsoft 365 applications should be prioritized over Google

applications.

- **Licensed Third-Party Apps Exception:** To maximize the utility of the University's digital resources while adhering to security and compliance standards, Illinois Tech allows for exceptions when the University holds licenses for third-party applications that provide functionalities that are not available in previously approved applications.
- **Prohibition of Unlicensed Third-Party Applications: To** ensure data security and uniformity in the University's digital environment, the use of third-party applications is prohibited if approved applications offer similar functionality. Any exception must be specifically licensed by Illinois Tech and approved for use by OTS as outlined below.
- **Exceptions Process:** Requests to integrate with Microsoft 365 and Google applications require formal review by OTS for approval or denial. Requests will be reviewed upon submission of the following:
    - Written justification documenting the needs not met by Illinois Tech-licensed applications
    - A cost estimate for the proposed tool
    - The party within the department responsible for implementation and troubleshooting
    - A timeline for implementation
      Estimated labor hours for OTS and the requesting department to implement the tool
    - Signature of the department administrator authorized to approve the expenditure

Recordings and Transcriptions

- Under applicable Illinois law(s) regarding eavesdropping and wiretapping, all parties to a conversation, whether in-person or via electronic means (whether audio only or audio with video), must expressly consent in advance for a conversation to be recorded. If even one party does not consent, the conversation may not be recorded. Surreptitiously or secretly recording a conversation is a violation of Illinois law that can result in both civil and criminal liability.
- **Voice Recording**: Participants must explicitly consent before any recording of voice, video, or written communications, regardless of the platform. Communication initiators must notify participants of intent to record ensuring a conspicuous and documented notification.
- **Transcription Purpose Disclosure:** Assuming all parties have consented to the recording of a conversation, if the conversation will be transcribed, all parties must be informed in advance of the purpose and scope of the transcription, how the transcript will be used, who will have access to it, and how long it will be retained.
- **Text-based Transcription**: Before initiating any form of text-based transcription of conversations, whether manual, electronic, or through artificial intelligence (AI) technologies, explicit consent must be obtained from all participating parties. This includes, but is not limited to, meetings, phone calls, video conferences, and in-person discussions.
- **Method of Obtaining Consent**: Written consent should be acquired wherever possible, especially in formal or recorded settings. If not able to obtain written consent, verbal consent

must be secured before starting the recording, and confirmation of verbal consent should be documented in writing as soon as practicable after the conversation ends. As stated above, recording is prohibited under Illinois law if any participant objects, whether they state their objection verbally or in writing. For impromptu or informal conversations, verbal consent is permissible, but must also be clearly documented. Consent should be obtained each time a conversation is to be recorded or transcribed, unless ongoing consent is given for recurring events (e.g., weekly meetings), and is documented in advance.

- **Right to Withdraw Consent:** Participants have the right to withdraw their consent at any time. In such cases, recording or transcription must cease immediately, and any transcribed material up to that point should be handled according to data privacy regulations and University policies.
- **Usage of Recordings and Transcriptions:** Recordings and transcriptions of communications are strictly for agreed upon use, explicit written consent is required for any other use or purpose. Non-participants seeking access to recordings or transcripts need consent from all parties.
- **Data Privacy and Security**: All recordings and transcribed material must be stored, handled, and disposed of in accordance with Illinois Tech's policies, plans and standards. Access to recordings and transcripts should be restricted to authorized personnel only.
- **Ramifications of non-compliance:** Violations of these guidelines may result in disciplinary action as outlined by any Illinois Tech policies, plans, and standards with potential legal implications under statute. Violations are to be reported to the Office of General Counsel.

Artificial Intelligence (AI)

- Users must employ AI technologies in a responsible manner, abstaining from any discriminative behavior or harming individuals. Users should ensure that the development and deployment of AI aligns with principles of academic integrity and respects the privacy and data rights of all individuals impacted.
- Users must not share any Confidential Data or Internal University-related Data with unsanctioned AI platforms. This includes, but is not limited to, research data, administrative data, and any form of PII. Furthermore, this prohibits sharing University-related data with AI-based chatbots, data analytics tools, machine learning platforms, and any other AI systems not explicitly sanctioned by Illinois Tech.
- All users are responsible for protecting any data that they create or handle. Users must not input, upload, or otherwise expose any Confidential Data or Internal Data to unsanctioned AI platforms.

- Users must provide appropriate disclosure on their use of AI technologies when used to hold communications with humans, in a research setting, or when AI output can be mistaken for human-generated content.

  Note: Refer to "Consent for Recording and Transcriptions" section for the use of AI transcription.
- Users must align with Illinois Tech's Data Governance Guidelines when handling data with AI technologies, including provisions for privacy, security, and ethical usage.
- Using AI to develop intellectual property must follow the Illinois Tech's Intellectual Property Policy for owning and using ideas or inventions.
- Users are encouraged to pursue training for ethical challenges and responsibilities related to AI use.
- Alleged violations are to follow the Sanction procedures outlined below. Users must report misuse or abuse of AI technology to the Office of General Counsel.

Cybersecurity Awareness Training

- To maintain a valid user account to access the University's Technology Resources, all users must satisfactorily complete Cybersecurity Awareness Training initially when granted access and annually.
- In the case of Simulated Phishing failure, users must complete additional Cybersecurity Awareness Training as defined by CTS.

Sanctions

- Access may be suspended with or without notice when continued use of these resources may interfere with the work of others, place Illinois Tech or others at risk, or violate federal, state, or local laws. This includes those related to copyright protection and Illinois Tech policy.
- Sanctions for non-compliance may include, but are not limited to:
  - Suspension and termination of access, up to and including termination of employment or enrollment
  - Formal disciplinary procedures in accordance with Illinois Tech's policies and procedures
  - Legal action for violation of civil or criminal laws, regulations, and/or contractual requirements
  - Confiscation of devices, computers, networking equipment or any other non-compliant hardware and software
- Some examples of non-compliance:
  - Failure to complete required Cybersecurity Awareness Training
  - Repeated failures of Simulated Phishing

- Mishandling of PII, up to and including ePHI
- Unauthorized installation of network or computing devices such as hardware and software

Responsibility

It is the responsibility of all Illinois Tech's users to ensure compliance with this policy, and to ensure external vendors working on their behalf comply.

Violations

Illinois Tech investigates and responds to all reports of violations of this and other related policies. Violation of policies will result in disciplinary action in accordance with the Acceptable Use Policy (AUP) and as determined by organizational leadership. If you have any questions about this policy, please contact CTS@iit.edu.

Review

Review of this policy will be completed on an annual basis or as needed to ensure the applicability of this policy to the changing environment.