

# HUCK-IT-P001: Acceptable Use



## On this page:

- [1.0 Overview](#)
- [3.0 Scope](#)
- [4.0 Policy](#)
  - [4.1 General Use and Ownership](#)
  - [4.2 Security and Proprietary Information](#)
  - [4.3 Unacceptable Use](#)
    - [System](#)
    - [Network Activities](#)
    - [Communications](#)
    - [Activities](#)
- [5.0 Enforcement](#)
- [6.0 Supporting Documents](#)
- [Glossary](#)

## 1.0 Overview

The purpose of this document is not to impose restrictions that are contrary to the Pennsylvania State University's established culture of openness, trust and integrity. The Huck Institutes of the Life Sciences is committed to protecting our employees, partners and the University from illegal or damaging actions by individuals, either knowingly or unknowingly.

## 2.0 Purpose

The purpose of this policy is to outline the acceptable use of technology resources that are managed by the Huck Institutes of the Life Sciences at the Pennsylvania State University. These rules are in place to protect anyone that utilizes resources that are managed by the Huck Institutes of the Life Sciences IT department. Inappropriate use exposes the Huck Institutes of the Life Sciences and the Pennsylvania State University to risks including virus and malware attacks, compromise of network systems and services, data loss or contamination and numerous potential legal issues.

## 3.0 Scope

This policy applies to any person who utilizes technology resources that are managed by the Huck Institutes of the Life Sciences or to any person who handles data that is the property of Pennsylvania State University by utilizing Huck Institutes' resources. We encourage you to read "HUCK-IT-P000 Introduction to Information Security at the Huck Institutes of the Life Sciences" for a primer on the philosophy adopted as part of the management of information at the Huck Institutes of the Life Sciences.

The policy augments the following Pennsylvania State University policies:

- [AD95 Information Assurance and IT Security \(Formerly AD20\)](#)
- [AD96 Acceptable Use of University Information Resources](#)
- [AD11 – University Policy on Confidentiality of Student Records](#)
- [RPG01 - The Responsible Conduct of Research \(Formerly RAG16\)](#)
- [FN14 Use of University Tangible Assets, Equipment, Supplies & Services](#)

## 4.0 Policy

### 4.1 General Use and Ownership

- While the Huck Institutes of the Life Sciences IT department desires to provide a reasonable level of privacy, users should be aware that the data they create on systems that are owned or managed by the Pennsylvania State University remains the property of the Pennsylvania State University unless an alternative agreement is in place. Additionally, data that is created on personally-owned devices as part of Pennsylvania State University contract work also remains the property of the Pennsylvania State University. Because of the need to protect Pennsylvania State University networks, systems and data, the Huck Institutes of the Life Sciences cannot guarantee the confidentiality of information stored on any network device belonging to the Pennsylvania State University. [RPG01, AD23]
- End users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning the personal use of network-connected systems. In the absence of such policies, end users should be guided by University policies on personal use, and if there is any uncertainty, employees should consult their

supervisor or manager. The Huck Institutes IT department strongly recommends that no personal usage be allowed on devices that process critical data or that connect to important instruments. [AD20, FN14]

- Users whose accounts are managed by the Huck IT department must sign a "User Agreement" form confirming that they have read and understand University Policies AD11, AD20, AD23 and ADG02 as well as Huck Institutes of the Life Sciences policies before accounts will be activated and network access will be granted. [ADG02, HK]
- The user agrees not to attempt to obtain or view any institutional data that is not intended for use in her/his job function or for which they do not have a "need to know". [RPG01, AD20, AD23]
- Authorized officials of the Pennsylvania State University may monitor equipment, systems, data and network traffic at any time. [AD20]
- No personal data processing devices will be connected to the wired network infrastructure managed by the Huck Institutes IT staff. Personal data processing devices may be connected to the Penn State wireless network infrastructure. [HK]
- All software installed on university-owned equipment must be properly licensed and must be used in accordance with the software vendor's license agreement(s). All software and licenses are subject to college and university audit. [AD20]
- Computers purchased through the Pennsylvania State University, including those that are grant funded, are considered university assets and as such are accountable as inventory through the user's budgetary unit. [FN14]
- The user understands that access to equipment, systems, data and networks that are owned or managed by the Huck Institutes of the Life Sciences constitutes his/her continued agreement with the Huck Institutes of the Life Sciences and Pennsylvania State University policies. If the user chooses not to comply with these policies, s/he will cease using their access account and immediately notify the Huck Institutes of the Life Sciences IT staff or appropriate university authorities. Upon receipt of notification, the user's account(s) will be disabled. Accounts managed by the Huck IT department will be terminated in three (3) months if no further communication regarding the status of the account is received. Data will be deleted after one (1) year. [ADG02]

## 4.2 Security and Proprietary Information

- All Huck Institutes owned devices that store proprietary data or that transport proprietary data must implement a secure authentication and/or access control process. All devices that do not support authentication and/or access control and that store or transport proprietary data must implement encryption as required by the data owner. [RPG01, AD20, AD23, MSB]
- All services managed by Huck Institutes staff and that provide a user interface for access to proprietary data must display warning text describing the highest classification level of the data that the service may provide. Managers of these services should take all necessary steps to prevent unauthorized access to the data provided by the service.
- Physical access to proprietary data storage or transport devices must be strictly controlled. Auditing of physical access should be enforced whenever possible. [MSB]
- All passwords and accounts should be secured and not shared. Authorized users are responsible for the security of their passwords and accounts. [AD20, ADG02, MSB]

## 4.3 Unacceptable Use

Under no circumstances is an end user of resources or data managed by the Huck Institutes of the Life Sciences authorized to engage in any activity that is illegal under local, state, federal or international law. The following activities are prohibited except for certain exemptions as identified under Section 4.1, General Use and Ownership or specified in other Huck Institutes of the Life Sciences policies. The list is not exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

### System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Pennsylvania State University.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Pennsylvania State University or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Pennsylvania State University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Pennsylvania State University account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior agreement with the Huck Institutes of the Life Sciences IT staff is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty and an agreement is in place with the Huck Institutes of the Life Sciences IT staff.
- Circumventing user authentication or security of any host, network, device or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Pennsylvania State University employees to parties outside of Pennsylvania State University.

## Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via electronic communications whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Pennsylvania State University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Pennsylvania State University or connected via Pennsylvania State University's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Holders of Pennsylvania State University's confidential and/or proprietary information are prohibited from revealing that information when posting to public sites or services.
- End users may not engage in any posting that may harm or tarnish the image, reputation and/or goodwill of the Huck Institutes of the Life Sciences or Pennsylvania State University. End users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when posting or otherwise engaging in any conduct prohibited by Pennsylvania State University's Non-Discrimination and Anti-Harassment policy.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the Huck Institutes of the Life Sciences and Pennsylvania State University trademarks, logos and any other intellectual property may also not be used in connection with any posting activity.

## 5.0 Enforcement

Any employee, student or visitor found to have violated this policy may be subject to revocation of privileges as well as disciplinary action by their Administrative unit, the College, or the University.

## 6.0 Supporting Documents

- HUCK-IT-P000: Introduction to IT Services at the Huck Institutes of the Life Sciences
- HUCK-IT-P002: Data Protection
- HUCK-IT-P003: Authentication and Access Control
- HUCK-IT-P004: Remote Access

<b>Glossary</b>	
<b>Network</b>	Wired or wireless infrastructure that provides for the exchange of data.
<b>End User</b>	A person who uses a device or service provided by university IT entities
<b>Information Security</b>	Information can be any type of knowledge or content that is used by oneself or communicated to others. Information does not have to be valuable in and of itself but can contribute to the overall value of the organization when combined with other information. Security is the assurance of safety through the reduction or elimination of risk. Put together in the context of the Huck Institutes of the Life Sciences, "Information Security" is the protection of the value of the organization through the reduction of risk to the knowledge or content that contributes to that value. Note that "Information" and "Data" can be used interchangeably throughout these policies.
<b>Service</b>	A combination of people, processes and technology that support business operations
<b>System</b>	Any university-owned computing devices, either stand-alone or connected to university networks.

Visit the Huck Institutes of the Life Sciences on the web at <http://www.huck.psu.edu>.

This publication is available in alternative media on request.

*The Pennsylvania State University is committed to the policy that all persons shall have equal access to programs, facilities, admission, and employment without regard to personal characteristics not related to ability, performance, or qualifications as determined by University policy or by state or federal authorities. It is the policy of the University to maintain an academic and work environment free of discrimination, including harassment. The Pennsylvania State University prohibits discrimination and harassment against any person because of age, ancestry, color, disability or handicap, national origin, race, religious creed, sex, sexual orientation, gender identity, or veteran status and retaliation due to the reporting of discrimination or harassment. Discrimination, harassment, or retaliation against faculty, staff, or students will not be tolerated at The Pennsylvania State University. Direct all inquiries regarding the nondiscrimination policy to the Affirmative Action Director, The Pennsylvania State University, 328 Boucke Building, University Park, PA 16802-5901; Tel 814-863-0471/TTY.*