HUCK-IT-P002: Data Protection and Retention

On this page:

- 1.0 Overview
- 3.0 Scope
- 4.0 Policy
  - 4.1 Philosophy
  - 4.2 Data Categorization
  - 4.3 Responsibility
  - 4.4 The Huck Minimum Security Baseline
  - 4.5 Software Installations
  - 4.6 Huck-Owned End-User Devices
  - 4.7 Data Storage and Backups
  - 4.8 Media
  - 4.9 Personal Devices
  - 4.10 Network Device Registration
  - 4.11 Network Scanning
  - 4.12 Lab Networks
  - 4.13 Reporting
  - 4.14 Best Practices
  - 4.15 Data Retention
- 5.0 Exceptions
- 6.0 Enforcement
- 7.0 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.

Ultimately it is data that is critical to the functions of the Pennsylvania State University that must be protected no matter where it resides. Devices that are owned by the University are to be used for business purposes in serving the interests of the university and of our clients and customers in the course of normal operations. Please review applicable Penn State policies for further details.

Effective security is a team effort involving the participation and support of every Penn State employee and affiliate who deals with data and/or data processing systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the protection and retention of data that is created, collected, or manipulated by personnel that fall within the scope of the Huck Institutes of the Life Sciences at the Pennsylvania State University. Improper handling of data 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 resources that are managed by the Huck Institutes of the Life Sciences or to any person who handles data that is the property of the Pennsylvania State University by utilizing Huck Institutes' resources. We encourage you to read "HUCK-IT-P000 Introduction to IT Services 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.

This policy augments the following Penn State University policies as well as additional applicable policies:

- **AD95 Information Assurance and IT Security (Formerly AD20)**
- **AD96 Acceptable Use of University Information Resources**
- **AD11 – University Policy on Confidentiality of Student Records**
- **AD35 – University Archives and Records Management**
- **General Retention Schedule (Formerly Appendix 18)**
- **Government Policies – HIPPA and FERPA.**

4.0 Policy

4.1 Philosophy

One way that Information Security can be fundamentally broken down is into three elements making up a useful model frequently called the "CIA Triad". The "CIA Triad" is probably the most widely accepted foundational model for Information Security at this time. "CIA" in this case does not stand for "Central Intelligence Agency", but instead stands for "Confidentiality, Integrity and Availability":

Confidentiality can be defined as preventing the disclosure of information (data) to entities that are not authorized to have access to that data.

Integrity can be defined as ensuring that data cannot be modified, including deleted, by unauthorized parties and also ensuring that improperly modified data can be restored.

Availability can be defined as ensuring that data is accessible when it is needed.

The Huck Institutes of the Life Sciences is using the "CIA Triad" as the foundation for its information security practices and procedures and we recommend those affiliated with the Huck Institutes do the same.

- You can meet Confidentiality requirements by ensuring that information is only made available to those who are authorized to have access to that information and nobody else ("need to know").
- You can meet Integrity requirements by ensuring that those who have access to information only have the specific level of access (e. g., read-only, write, delete, etc.) that they need and no more.
- You can meet Availability requirements by ensuring that information is protected from unexpected loss.

University policies regarding data protection and retention as listed in this document are not exhaustive, but rather serve as a foundation that resource administrators and data stewards will build upon to ensure that information is adequately protected. Before working with data, it is important that data stewards understand who the owner of that data is and what requirements the owner of the data has in place to ensure that the data is adequately protected by anyone who has access to it. Data owner requirements may exceed University requirements for data protection.

Huck Institutes of the Life Sciences staff are expected to follow the data protection requirements outlined in this policy document which at a minimum requires that Penn State's Data Categorization policies are followed and that the associated Minimum Security Baseline requirements are met.

4.2 Data Categorization

Penn State requires an adherence to Policy AD71 Data Categorization by anyone who handles data in any way. This policy identifies three categories of sensitivity with regard to data used within the University:

- Public
- Internal/Controlled
- Restricted.

Policy AD71 also references additional policies and guides that provide further details on the proper use, handling and classification of various types of data.

4.3 Responsibility

If you are the designated owner of data, then you must make a determination as to the proper classification and handling of that data while understanding external requirements such as sharing research data, export controls, ITAR, etc. If you are the manager or steward of data, then you must adhere to someone else's requirements as to the proper handling of that data. In either case, you should use Penn State Policy AD71 and other data categorization tools that the University provides as the foundation for your data management plan.

As the owner and/or manager of data, it is your responsibility and your responsibility alone to ensure that you are protecting that data to a level that is commensurate with its importance. Although you are using resources provided by the Huck Institutes, you must either work with qualified Huck or University staff to meet data protection requirements or you must ensure that the resources necessary to meet those requirements are being provided if the Huck Institutes does not provide them.

You should make no assumptions about the security levels of resources that are provided by the Huck Institutes. If your data protection requirements have "need-to-know" constraints or require specific protections whether the data is at rest or in transit, then you yourself must ensure that you have implemented a data protection process that meets those requirements.

It is everyone's responsibility to report suspected data protection violations at a minimum to Huck Institutes IT or Administrative staff or Penn State Security Operations and Services. See the "Reporting" section later in this policy.

The Huck Institutes is not responsible for third party software or web applications that are developed and deployed by non-Huck staff. Any third party service or software that is hosted on Huck Institutes owned assets or university owned systems, must meet the University's Minimum Baseline Security requirements. We encourage you to consult with Penn State Security Operations and Services resources to ensure that your services are properly configured and that associated data meets minimum protections based upon its categorization.

4.4 The Huck Minimum Security Baseline

Any data processing or storage device that is connected to the Penn State backbone via a wired connection in Huck Institutes facilities is required to meet University policy requirements. Systems that are owned by the Huck Institutes of the Life Sciences will be configured with the following products.

Product	Required	Optional	Notes
Endpoint Protection	Windows; Mac OS; Android; Linux		University required; Managed required for Huck-owned devices; weekly scans at a minimum unless exception granted.
Anti-Malware	Windows	Mac OS; Linux; Android	Required for Windows-based Huck-owned devices; Highly recommended for non-Huck devices.
PII Audit	Windows; Mac OS		University required.
Firewall	Windows; Mac OS; Linux		Highly recommended; Configured by default for Huck-managed devices; Can be provided by Endpoint Protection product(s).

More details are provided in **HUCK-IT-S001 Device Standards for Meeting University Data Protection Requirements** and **HUCK-IT-G001 Device Lifecycle Management**.

4.5 Software Installations

- No initial software installations should occur on Huck Institutes-owned systems without first coordinating with the Huck Institutes IT staff.
- All software distribution sources must be verified as safe and secure before they may be used to download and/or install software.
- All software must be used under the terms outlined in the product's licensing documentation and/or terms of use agreement.

4.6 Huck-Owned End-User Devices

- Devices should be configured with an automatic screen lock with a password required to regain access. Devices should be manually locked, and preferably logged out, before leaving the vicinity of the device for any period of time.
- Power management settings should be configured to optimize usage and power savings. Devices should not be left running all the time unless there is a specific requirement for them to do so.
- Devices should primarily be used for business purposes. There is an expectation that some access to personal services from the business device will occur. This access should be kept to a minimum and the end user assumes all risk when accessing a non-business service from a business device.
- Food and drink should be kept away from devices.
- Displays should be positioned away from public view.
- All AC power connected devices should be connected to a surge protector at a minimum, but preferably a UPS so that the potential for uncontrolled shutdown is significantly minimized.
- Devices should not be used to host critical services or data.
- Staff devices will not be automatically backed up by default.

4.7 Data Storage and Backups

- Institutional data should be stored on file servers maintained and backed up by Network Operations. The backup mechanism for Network Operations is Tivoli Storage Manager (TSM) provided by ITS.
- Personal data should be stored on PASS or an approved online storage service.
- Important data that resides on servers that are managed by Huck IT staff will be backed up once in every 24 hour period. Backups will be retained for at least one month with longer retention periods available for critical servers.

4.8 Media

- No removable media devices shall be connected to systems without absolute confidence that the media is safe. If there is any doubt whatsoever, please coordinate with the Huck Institutes IT staff.

4.9 Personal Devices

- No personal devices are permitted on the wired network. Personal devices may only be connected to the Penn State wireless network. No support is provided for personal devices.

4.10 Network Device Registration

The following applies to any device regardless of its ownership status:

- Before any Penn State owned device is connected to the Penn State backbone via a wired connection in Huck Institutes facilities, that device must first be registered in the network information database maintained by the Huck IT staff. Registration can be accomplished by submitting a support request at https://home.huck.psu.edu/support.
- Once a device is registered in the network information database, any change in the device's status (including moves to another wall jack, device removal, etc.) should be reported to the Huck IT staff via a support request at https://home.huck.psu.edu/support.
- No user will attempt to connect any equipment to Huck Institutes networks unless authorized by a member of the Huck Institutes IT staff. No user may attempt to create a bridge to the Huck Institutes network without permission. Any bridges to the network will be considered an extension of the Huck Institutes network for the purposes of this policy.
- Twice annually, network administrators will remove from the registration database any previously registered device that has not authenticated in the prior six months.

4.11 Network Scanning

- Scanning and/or monitoring of network traffic is not permitted without the express written consent of the Huck Institutes Director or Assistant Director of Information Technology.

4.12 Lab Networks

- Lab owning organizations are responsible for assigning lab managers, a point of contact (POC) and a backup POC for each lab depending upon staff size. Lab owners should not be the POC unless absolutely necessary. Lab owners must maintain up-to-date POC information with the Huck Institutes IT staff. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions may need to be taken without their prior approval.
- Lab owners are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined, lab managers must do their best to safeguard Penn State from security and liability issues. If there is any doubt, please reach out to the Huck Institutes IT staff for support.
- The lab manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
- All lab equipment must sit behind a properly configured network firewall. If there is any question as to whether or not this requirement is met, please contact the Huck Institutes IT staff.
- The Huck Institutes IT staff and/or Penn State Security Operations and Services (SOS) reserve the right to interrupt lab connections that impact the production network negatively or that pose a security risk.
- Any lab that wants to add an external connection must provide a diagram and documentation to the Huck Institutes IT staff with justification, equipment and the IP address space information. The Huck Institutes IT staff will review the submitted information for security concerns and must approve the plan before such connections are implemented.
- Lab network devices must not cross-connect, or bridge, the lab and production networks.
- Any change to the security or firewall configuration of a lab-connected device must first be approved by the Huck Institutes IT staff before implementation.
- The Huck Institutes IT staff and/or Penn State Security Operations and Services (SOS) reserve the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network-connected peripherals.
- The administrator/root password for all lab-owned devices must be different from all other equipment passwords in the lab. This password will only be provided to those who are authorized to administer lab equipment.

4.13 Reporting

If you suspect that a data compromise may have occurred or if you identify a situation that could potentially lead to a data compromise, then it is your responsibility to report it. The following reporting structure should be followed with progression down the list if you feel that the entity you are reporting to is not responding adequately to the situation:

- Immediate Supervisor
- Huck IT
- Huck Administrative Staff
- Penn State Security Operations and Services

When Huck IT is made aware of a potential compromise, the potentially compromised device (or container) is removed from any network connectivity and seized. If Penn State Security Operations and Services is not already aware of the compromise, then a report is filed with them.

If the compromise is validated, then the system is fully scanned for any Personally Identifiable Information (PII) or other critical data and a report is submitted to the SOS group. Once mitigation instructions have been provided by SOS, the system is wiped and either rebuilt or returned to its manager. Post-rebuild, the system must meet the Huck Institutes Minimum Security Requirements as outlined in "Container Protections" before being allowed to reconnect to any networks.

4.14 Best Practices

We are including some best practices merely as guidance for certain common scenarios. These are not all inclusive and you are encouraged to contact Huck Administrative or IT staff if you have specific scenarios that you would like to address.

- We recommend that no critical data be permanently stored on end user devices. As much as possible, data should be stored on access-controlled servers located in physically secure data centers or computer rooms.
- We recommend no extraneous processing be performed on systems that directly interact with critical research equipment. Extraneous processing could include: general Internet browsing, sending/receiving of electronic communications,

streaming from public networks, etc. In fact, it is highly recommended that systems that collect or process data from research equipment be segmented from any public networks and that any critical data that they manipulate be backed up as quickly as possible.

4.15 Data Retention

AD35 - University Archives and Records Management references the General Retention Schedule (previously Appendix 18) which in turn contains a table specific to "Grant and Contract Records". This table lists "Scientific and Technical Data" as having a retention policy of "3 years in Office; Transfer to Archives for PERMANENT file." The Huck Institutes does not have the resources to provide permanent retention for all research data nor do we provide storage services to non-Huck personnel.

5.0 Exceptions

Exceptions to policies can only be evaluated by completing form HUCK-AD-F001: Request for Policy Exception or Exemption. This form must be fully completed and signed by either the Director of the Huck Institutes or the Director of Administration for the Huck Institutes or their designees.

6.0 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.

7.0 Supporting Documents

- HUCK-IT-P000 Introduction to IT Services at the Huck Institutes of the Life Sciences
- HUCK-IT-P001 Acceptable Use
- HUCK-IT-P003 Authentication and Access Control HUCK-IT-P004
  Remote Access
- HUCK-IT-S001 Device Standards for Meeting University Data Protection
- Requirements HUCK-IT-G001 Device Lifecycle Management

Glossary	
Network	Wired or wireless infrastructure that provides for the exchange of data.
End User	A person who uses a device or service provided by university IT entities.
Information Security	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.
Service	A combination of people, processes and technology that support business operations.
System	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.