HUCK-IT-G001: Device Lifecycle Management

On this page:

1.0 Overview
3.0 Scope
4.0 Policy
4.1 Product Research
4.2 Procurement
4.3 Deployment
4.3.1
Risk Reduction
4.3
4.3
4.4 Device Retirement
5.0 Exceptions
6.0 Enforcement
7.0 Supporting Documents

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 checklist is to provide guidance as to how devices should be procured, managed and disposed of in order to meet Pennsylvania State University policies and recommended practices. This checklist will be as generic as possible and therefore it will not include step by step instructions for the implementation of each recommendation. Device managers are encouraged to use University and third-party resources as much as possible to implement these recommendations. Huck IT only provides technical support to Huck staff for Huck-owned devices. Personnel who are not Huck Institutes staff should coordinate with their home IT departments as much as possible in order to make this process flow more smoothly.

3.0 Scope

This checklist can be used by personnel who are involved in the configuration and management of devices that perform computational or storage processing in facilities managed by the Huck Institutes of the Life Sciences. This checklist assists in the mapping of configurations and practices to University policies and recommendations.

The following list of applicable policies is provided as a reference:

- **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 Product Research

As you begin to evaluate products that you may be introducing to the University environment, there are many items to consider, such as:

- Will the device meet Penn State University requirements specific to the handling and processing of data? Please see Penn State's Data Categorization Project web site. Also, the Minimum Security Baseline Home wiki space details more specific requirements and associated controls.
- Will the device operate within the confines of Penn State University policies?
- If the device runs an operating system, is that operating system still supported?
- Have environmental considerations been taken into account? Noise levels?
- Does the physical space that is planned to home the device have the infrastructure systems in place to support it?

- Electrical
- Networking
- Plumbing
- Interference mitigation
- Physical security
- HVAC

A good starting point is to contact your home unit's Facilities and IT groups who should be able to provide some direct answers or point you in the right direction for additional help.

4.2 Procurement

When requesting a quote from a vendor, provide them with a checklist of the basic requirements for operating the device at Penn State. Vendors cannot mandate requirements that override University requirements without a mutually agreed upon compensating control being in place before the system is procured.

Review the Penn State purchasing site for the process that must be followed and the forms that must be submitted for the procurement action that you are taking. As an example, the University requires a review of software agreements via a form submission before completing a procurement. This is to ensure that the vendor's licensing terms do not legally bind the University to actions to which it cannot comply.

Your home unit's administrative staff should be able to provide guidance for navigating the procurement process.

4.3 Deployment

Most IT groups have a standard process that they use for new device deployments. Submit a request through your home IT group's issue /request mechanism to get their assistance with your device deployment. Please understand that your home IT group may have a significant number of open issues that they are addressing on a daily basis, so they may not be able to immediately respond to your deployment request.

If the device will ultimately connect to a wired network managed by Huck IT, then a separate network connection request, providing detailed information (including the MAC addresses of devices to be connected), must be made through the Huck Service Desk. Huck IT will verify that the device has been managed by the requestor's home IT unit before registering it for network connectivity.

4.3.1 Risk Reduction

Perhaps the most important deployment step for any device is risk reduction. This section contains a checklist of common risk reduction items that can be used to help the device owner meet many of Penn State's baseline requirements.

4.3.1.1 Configuration

Configuring a device within the scope of this checklist means that you are making changes so that it can meet the requirements of the environment under which it operate. In most cases at Penn State, this means that you are modifying your device so that it can operate on University-provided networks and with stronger defenses in place than those of an out-of-the-box device. The Minimum Security Baseline Home wiki space outlines which controls are required depending upon the type of data processed by the system.

Note: References to Windows in these tables are the business versions of the operating system.

Install Antivirus software and keep it up to date. Enable real time protection. Schedule periodic scans.	Penn State provides Symantec Endpoint Protection for Windows and Macs at https://downloads.its.psu.edu. Penn State also provides access to a console for centralized management. Your home IT group may have more information.
Install/configure a local firewall.	OS X 10.5.1 and higher and Windows XP and higher as well as most Linux distributions include basic firewall functionality built-in. Penn State provides Symantec Endpoint Protection for Windows and Macs at https://softwarerequest.psu.edu/.
Install Anti-Malware software and keep it updated. Enable real-time protection. Schedule periodic scans.	Highly recommended for Windows and Macs. Penn State does not currently provide a specific product, but some departments/units might. Please check with your home IT group.
Critical file backups.	Modern versions of Windows, OS X and Linux include file level backup tools. Additionally, scripts can be created using built-in operating system commands and automated to perform backups. It is very important to identify critical files that need to be backed up and it is just as important to ensure the backups are being performed and are complete. Penn State provides TSM at https://softwarerequest.psu.edu/. Please check with your home IT group.
System image backups.	Modern versions of Windows, OS X and Linux include system image backup tools. Penn State does not currently provide system image software. Please check with your home IT group.
Use a screen lock with a timer.	Modern versions of Windows, OS X and Linux provide screen lock features. An Internet search will lead to numerous articles describing implementation steps.
Encrypt mobile devices.	Modern versions of Windows, OS X and Linux include file and system encryption tools. An Internet search will lead to numerous articles describing implementation steps.
Install/configure Personally Identifiable Information scanning software. Schedule periodic scans.	Penn State provides Identity Finder for Windows and Macs at https://softwarerequest.psu.edu/.
Enable auditing.	Modern versions of Windows, OS X and Linux include auditing features, but some level of configuration may be required. An Internet search will lead to numerous articles describing implementation steps.
Retain critical logs.	Logs that must be retained should be available online for at least a month with the ability to recover the past year's logs upon request.
Install system and application updates.	Most operating systems include either automatic or manual update capabilities with notifications when updates are available. Many applications provide the same features. You should ensure that updates are installed on a regular basis (at least monthly) and install immediate out-of-band updates to resolve critical bugs and security issues.
Logon banners.	Logon banners should, at a minimum, display logon warnings/notifications (such as policy acceptance text) as well as information clearly identifying the owner of the system. An Internet search will lead to articles describing implementation steps.
Install system and application updates.	Most operating systems include either automatic or manual update capabilities with notifications when updates are available. Many applications provide the same features. You should ensure that updates are installed on a regular basis (at least monthly) and install immediate out-of-band updates to resolve critical bugs and security issues.
Enforce complex passwords and restrict configuration changes.	System and service level passwords should be configured to enforce complexity, extended length, multiple character classes and potentially be supplemented with additional authentication factors. Controls should be in place to prevent non-administrator level end- users from making changes to password policies and any policy changes should be audited and logged.

4.3.1.2 Practice

Practice within the scope of this checklist means that you are operating the device in such a way as to reduce the risk of device compromise and/or data loss.

Configuration	Notes
Use strong passphrases.	It is recommended that you use a passphrase instead of a password. Passphrases should be at least 12 characters long and preferably longer, include a mix of character types and doesn't use obvious substitutions (e.g., the number 0 instead of the letter "O"). Penn State has posted some guidance at http https://security.psu.edu/services/penn-state-accts/passwords/choose/.
Manual screen lock.	Manually lock your screen when walking away instead of always relying on the screen lock timeout. An Internet search for "manual screen lock" and your operating system (e.g., "OS X") will lead to numerous guides.
Operate in least privilege mode.	Your daily operations should be performed under a non-Administrator/root account. If you require elevated permissions for any functions, use a separate Administrator/root level account or a program such as sudo. Check with your home IT group for more information.
No group accounts.	User actions should be traceable to a single user. Therefore, group accounts should not be available unless absolutely necessary and even then, compensating controls should be in place to audit specific user activity (e.g., a system access logbook).
Document system changes.	A system change management log should be kept for critical systems at a minimum. This helps to track specific events that could be pointed to as having caused a failure.
Label systems for identification purposes.	If your Penn State devices are not labeled, check with your home IT group to find out if they have a labeling convention and will apply it to your devices. A labeling system helps in reporting problems and allows you to better identify systems in your workspaces.
Offsite backups.	In addition to critical file and system backups, consider having a duplicate copy of the latest backup offsite. These backups should be even better protected than the onsite backups with encryption and physical security controls in place.
Use encrypted flash devices.	When using a flash device to transfer files, always assume that protected data will be stored on the device and that host devices are compromised. Look for flash devices that support strong encryption and that are write-protectable. Only write to the flash devices from other devices that you are confident are not compromised.
Use an encrypted connection to Penn State services.	Ensure that your connections to Penn State services are encrypted and that nobody is watching your screen or you as you type. Browser-based connections should use SSL (https) and a VPN would be preferred. Contact your home IT group for more information.
Transfer files securely.	Penn State provides several secure file transfer utilities at https://softwarerequest.psu.edu/. Additionally, every current Penn State employee and student is eligible for a Box account with 50 GB of storage. Non-Person Accounts with a quota of 1 TB are available upon request.
Beware of untrusted networks.	If you use a mobile device that moves between Penn State and external networks, you should be extra vigilant when accessing Penn State services over those external networks. As much as possible, only use networks that are trustworthy, make sure your security software is up to date and use a VPN to access Penn State services. Consult with your home IT group for more guidance.
Limit Internet access on critical systems.	If you have systems that you consider critical to your operations, you should configure the system to only access external sites that are absolutely vital for basic operations. This is typically done via a network proxy device which can be configured by your network operations group or IT staff. All proxy connections should be logged as part of your auditing process.

4.4 Device Retirement

Unfortunately, most device owners simply discard a device when they believe it no longer proves useful to them. However, there are many steps that should be taken in place of a device simply being tossed aside, such as:

Ensure that no device component containing **any** University data is simply discarded. You must ensure that the component has either been securely wiped or that it is properly destroyed.

Contact the network administrators to let them know that the device no longer requires wired connectivity. This allows the network administrators to free up valuable resources for use by other end users.

Contact your home IT group to let them know that the device is ready for retirement. In many instances, the home IT group will have a specific process that they go through to ensure the device can be safely disposed of and they may even be able to dispose of the device for you.

Contact any property administrators to let them know that the device is ready for retirement.

Work with your home group's property and financial administrators to ensure that there are no special requirements for the device. As an example, some devices are required to stay in specific facilities for a certain number of years based upon the funds used to procure them.

It is strongly recommended you transfer your device to Penn State Surplus once all of the administrative requirements for disposal have been met. Specifically, the "Send to Surplus" section of their web site contains details on what they accept and how to proceed through the process. 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.

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

N/A

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.