## 21 Asset Inventory and Device Management

**Purpose**

The purpose of this policy is to define requirements for tracking <Company Name> logical and physical assets through their lifecycle from initial acquisition to final disposal. This policy supports the Data Classification policy which establishes a framework for classifying corporate and customer data based on its level of sensitivity, value, and criticality to <COMPANY NAME>

**Hardware and Software Standard**

An inventory process must be in place to support the discovery, management and replacement/disposal of all significant Hardware and Software assets. The inventory process should facilitate the identification and removal of any illegal or unauthorized software found in the <COMPANY NAME> environment. The inventory process must include the following:

* A listing that captures appropriate details of significant Information and Technology Assets under <COMPANY NAME> management or control, including Hardware and Software assets.
	+ Details should include a description of the type of asset, the make of the asset, technical specifications, license details, and versions of the software packages or operating systems.
* Items can be excluded from the inventory if they carry very low purchase/replacement costs (including time and labor needed to install and configure) and pose little or no risk to business operations or compliance status.
* Each significant asset is associated with an identifier, license, or tag so that it can be identified and tracked.
* Whether through depreciation, expiring leases or agreements, obsolescence/end of support, loss, or other reasons, the disposal/replacement of Hardware and Software assets must be tracked.
* A reporting function must support auditing and monitoring for IT compliance with this standard.

**Hardware and Software Replacement Exception Standard**

<COMPANY NAME> may be required to upgrade or migrate from a hardware system or software program due to security issues, inadequate performance, a vendor discontinuing support for a product, or other reasons. It may not be feasible in all circumstances to perform an otherwise required upgrade or migration in a timely manner, most commonly due to unavailable resources or an unfavorable migration/upgrade Risk Assessment.

Prior to attempting a migration or upgrade of any significant hardware or software system, the IT Department must assess the risks associated with such a move in consultation with the impacted information resource owner(s). If <COMPANY NAME> is not able to perform an otherwise required upgrade or migration in a timely manner, an Exception to the upgrade/migration/replacement requirement may be granted to allow continued use of the impacted system of software for a defined period if continued use of the system is not contrary to the terms of any applicable contracts or licensing agreements and an Exception Request is approved by the CISO.

**System Inventory Standard**

A system inventory process must be in place to support the technological management of critical business processes and to meet legal and regulatory requirements. The IT Department is responsible for collecting the necessary information for the inventory which includes:

* A unique identifier or name of the system.
* The owner of the system – typically, but not necessarily the information resource owner.
* A description of the purpose of the system and the role the system has in supporting critical business processes and in meeting legal or regulatory requirements.

**System Retirement Standard**

The information resource owner determines when a system no longer is needed or is obsolete and can be retired. If the system to be replace/retired supports mandatory legal and regulatory requirements of critical business process, the information resource owner must ensure that any replacement system can support these processes before the current system is retired.

Before retiring/replacing any system, data retention requirements for all data stored or managed by that system must be reviewed, and a plan for complying with all applicable data retention requirements must be developed and executed. This is particularly important for systems that manage data subject to legal/regulatory scrutiny. Any data subject to data retention requirements must be migrated to an appropriate destination and tested for appropriateness, completeness, accessibility and retrievability from the destination before the original data is deleted from the original system as part of the system retirement process.

**System Hardening Standards**

**Device Best Practices and Hardening Standards**

* Manufacturer-provided hardening and best practice guides will be employed to ensure all device installation is properly guarded from vulnerabilities and unauthorized attempts to access the systems.
	+ Center for Internet Security (CIS) benchmarks are utilized where possible for system hardening guidance. (https://www.cisecurity.org/cis-benchmarks/)
* Vendor supplied defaults, including usernames, passwords, and any other common settings that that may result in unauthorized attempts to access to the systems, will be changed in accordance with hardening guides.
* Insecure and unnecessary communication protocols are disabled.
* Local passwords, when required, will be randomly generated and securely stored in the approved password vaulting system.
* Current patches will be installed.
* Malware protection will be implemented.
* Logging will be enabled.
* Two-factor authentication should be used whenever available/supported on the device platform.

**Infrastructure Configuration and Maintenance**

**Internal Workstation and Server Patching**

* Operating system patches/upgrades are evaluated monthly.
* Operating system patches/upgrades are installed based on their criticality. Security critical patches/upgrades are installed within one month of their release at the latest, pending approval.
* Operating system patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
* Monthly, the IT department reviews all servers to ensure that they remain up to date and are properly patched.

**Internal Infrastructure Patching**

* Infrastructure (routers, switches, virtual hosts, etc.) patches/upgrades are evaluated as they come available from vendors.
* Infrastructure patches/upgrades are installed based on their criticality. Security critical patches/upgrades are installed within one month of their release at the latest, pending approval.
* Infrastructure patches/upgrades are reviewed and approved via a lab environment when possible/practical.
* Infrastructure patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
* When applicable, redundant systems are patched/upgraded one device at a time to ensure no impact to shared services.
* Networking hardware/software updates follow the regular change management procedures.

**Infrastructure Support Documentation**

* The infrastructure topology is documented in full by the IT Department. A network diagram is available to all appropriate service personnel and is kept current.
* The infrastructure topology is never shared with outside personnel unless properly sanitized of all IP addresses and any other sensitive information.
* Configuration standards for the setup of all infrastructure devices are in place and are formally documented as necessary.
* Configuration standards include a standard list of security hardening principles.
* Access to the network and communication devices is documented and reviewed on an annual basis to ensure that access remains appropriate. Logs are maintained as necessary.

**End Point Security/Threat detection**

* Controls are in place to restrict the use of removable media to authorized personnel
* Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).
* Antivirus and anti-malware tools are configured to automatically receive updates, run scans and alert appropriate personnel of viruses or malware.
* Antivirus and Anti-Malware tools automatically scan removable media and incoming files.
* Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data.
* Host based Intrusion Detection Systems and/or personal firewalls are configured to identify suspicious traffic and communications.
* A process for monitoring end-points for unauthorized software is instituted.
* Mobile devices with access to the institution’s data are centrally managed for antivirus and patch deployment.
* The institution wipes data remotely on mobile devices when a device is missing or stolen.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 07.a – Inventory of Assets
* 07.b – Ownership of Assets
* 07.c – Acceptable Use of Assets

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(5)(i) - Security Awareness and Training
* 164.310 (c) – Workstation Security
* 164.310 (d)(1) – Device and Media Controls

Version History

Number Published Author Description