CONE HEALTH	**Guideline:** ITS Technology Asset Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
System administrators

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with technology asset management, accountability, repurposing, and destruction.

Scope and Goals:
This procedure addresses the management and destruction of Cone Health's technology assets used for the creation, storage and transmission of covered information. The goals of this procedure are as follows:

- Identify technology assets and services that fall within the scope of this procedure.
- Define technology asset ownership.
- Define technology asset accountability requirements.
- Define technology asset maintenance requirements.
- Define requirements for sanitizing technology assets prior to repurposing.
- Define technology asset destruction requirements.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Responsible for revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Approve all sanitization and destruction techniques (i.e., software or hardware).
- Periodically reassess the ITS asset lifecycle program to ensure current technologies and practices are still valid and continue to meet industry accepted practices.
- Ensure the shredding vendor has the appropriate security controls in place to prevent information leakage and signs a business associate agreement.

Information and Technology Services (ITS):
ITS is responsible for, but not limited to, the following activities:

- Maintaining an accurate inventory of all accountable technology assets and the users that are authorized to use the assets (including workstations, server infrastructure, mobile devices, portable devices, and any other device or system that can store, process, or transmit organizational data).

- Ensure the whereabouts of technology assets containing covered information are properly tracked at all times.
- Ensuring the main asset inventory does not duplicate other inventories unnecessarily and ensures their respective content is aligned.
- Ensure technology assets are properly sanitized before repurposing or destruction.
- Create and manage a formal migration plan for replacing hardware and software that is no longer supported by a developer, vendor, or manufacturer.
- Providing a current inventory of assets containing covered information to the CIO, CISO, and the senior privacy official on a periodic basis, but no less than annually.

Technology Asset Identification:
Technology assets meeting one or more of the following criteria will be considered an accountable technology asset:

- Devices that process, store or transmit covered information. This includes, but is not limited to, desktops, servers, laptops, smartphones, tablets, business machines, medical devices, and portable media (i.e., removable hard-drives, backup tapes, CDROMs, thumb/flash drives, etc.).
- Network equipment (routers, switches, firewalls, etc.)
- Voice over-IP telephones, multi-homed addresses, and virtual addresses.
- Capitalized technology assets will include all items with a useful life greater than one year, and a “unit purchase price” greater than $2,500, or a “grouped purchase price” greater than $5,000. Exceptions to the purchase rule include personal computer monitors, printers, software and the personal computer chassis. These will always be tracked in an effort to provide adequate inventory control for these items.
- Personally owned devices approved by the organization to store, process or transmit covered information.
- The following technology components (typically costing less than $500) will be capitalized only if included in the purchase of a personal computer system and shall be expensed if such components are purchased at a later date:
  - Network interface, modem, sound, graphics, and expansion cards
  - Media drives (e.g., hard-disk drives, CD-ROMs)
  - Keyboards, cables, mouse-type devices
  - Additional memory (RAM)
  - Software
- Volume purchases of identical items (e.g., RAM memory chips, software licenses) may be capitalized if the unit cost of the items on a specific invoice is at least $500 and the number of identical items times the unit cost equals or exceeds $1,000.

Technology Asset Ownership:
All technology assets are the property of Cone Health. Leased or otherwise externally assigned technology assets are still considered property of the Cone Health in accordance with the lease agreement and are required to comply with this procedure.

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Personally owned technology assets authorized for use in the workplace are accountable in accordance with this procedure and the Personal Device Use procedure.

Technology Asset Accountability:

ITS is responsible for conducting an annual inventory of all accountable assets and services. At a minimum, technology assets will be tracked and accounted for under the following criteria:

- Technology asset (physical) location
- Technology asset owner (name, manager's name, department and contact information)
- Technology asset tag number (with exception of personally owned devices, which will be tracked by owner name)
- Type/classification of covered information stored or could be stored on it (see Data Classification and Handling procedure)
- Identifies the types of protection required for the asset.
- License information
- Backup information
- Value (with exception of personally owned devices)
- Business criticality
- Technology being used off-premise

The purpose of the technology asset inventory is to ensure:

- Accountable technology assets are being properly accounted for
- Technology assets requiring periodic maintenance are identified
- Compliance with regulatory (i.e. HIPAA) requirements for technology assets containing covered information
- Property tax obligations
- Proper destruction requirements for technology assets containing covered information

ITS will maintain an accurate inventory/accounting at all times. ITS will update the technology asset inventory as changes occur. Events that require an inventory update are:

- Trade-in or turn-in of leased technology assets
- Lost or stolen technology assets
- Internal repurposing (i.e., reissue)
- Sale or donation of technology assets
- Obsolete technology assets
- Damaged technology assets that cannot be repaired
- Lending of technology assets (i.e., contractors, consultants, visitors, etc.)

For the purposes of tracking mobile devices, either employee or company owned, Cone Health utilizes a mobile device management (MDM) platform. The MDM platform is used to:

- Keep an inventory of all mobile devices.
- Identify who holds ownership of the device (personal or Cone Health).
- Allow for remote software version/patch validation.
- Wipe all Cone Health or customer data in the event the device is stolen, lost, or the workforce member terminates employment.

- Document and enforce a list of approved application stores acceptable for mobile devices to use. (also refer to the Personal Device Use procedure).
- Enforce password and authentication requirements and prohibit tempering with these policies.
- To detect and correct any altered baseline security configuration standards (as defined in policy) such as rooting or jailbreaking.

Technology Asset Maintenance, Repurposing, and Disposal:
Before repurposing (i.e., re-issuing) an accountable technology asset, all covered information must be removed in accordance with this procedure's sanitization requirements.

Before maintenance or repair of an accountable technology asset, all covered information must be removed in accordance with this procedure's sanitization requirements unless explicitly authorized otherwise by Cone Health's CISO. After maintenance or repair, all security controls must be checked and verified that they are active.

Destruction of technology assets containing covered information will be done in accordance with federal and state law and pursuant to the organization's written retention policy/schedule. See Sanitization Requirements below for approved techniques.

Technology assets containing data involved in any current or pending investigation, audit or litigation will not be destroyed. The following rules apply for these situations:

- Sanitization or destruction shall be suspended until such time as the situation has been resolved.
- In the event technology assets containing data are subpoenaed or requested by an outside party as a part of an investigation, audit, or litigation, a qualified protective order will be obtained to ensure that the technology assets are returned to the organization or properly destroyed/disposed of by the requesting party and destruction documentation will be provided to Cone Health.

Technology assets scheduled for decommissioning and destruction will be secured against unauthorized or inappropriate access until the technology asset has been properly sanitized or physically destroyed.

Sanitization Requirements:
Standard sanitization approaches include one of the following methods:

- Using approved software to overwrite the technology asset's memory using one of the following sanitization techniques:
  - Perform sanitization using approved software/hardware and use a Certificate of Destruction-Sanitization to record the action taken.
  - Outsourced sanitization using an onsite shredding service.
- Degauss the technology asset.

Technology assets that cannot be sanitized due to damage or non-functional status, or that are otherwise not writeable, must be destroyed in accordance with this procedure.

Sanitization guidance for specific technology asset types to include personally owned devices is as follows:

Portable Media: Due to the low-cost and short life of portable media, repurposing portable media is not authorized.

Hard-drives: Computer with fixed/removable drives (including external portable hard-drives) will be reset to the manufacturer's factory default settings and then sanitized. Examples of devices with hard-drive storage include, but are not limited to, tablet computers, computers/servers, network storage, printers, network devices (e.g., routers, firewalls).

Handheld Devices: Erase contents from the device following the manufacturer's instructions and then perform a full manufacturer's reset back to the factory default settings. Examples of hand-held devices include, but are not limited to, radios, dictation and recording devices, cameras (still, video), cell phones, smart phones, personal digital assistants (PDAs), barcode or smartcard readers, handheld printing devices (e.g., receipts, tickets, asset tags), media players, mapping/navigation devices, etc.

Destruction Requirements:

If a technology asset cannot be sanitized, the following will be done:

- Destruction by a certified shredding service; or
- Cone Health will physically destroy portable media and technology asset hard drives by any physical means that prevents reuse or data recovery.

Use a Certificate of Destruction-Sanitization to record action taken.

Technology Asset Retirement and Migration Requirements:

In the event where hardware and/or software used to store, process, or transmit covered information is no longer supported by a developer, vendor, or manufacturer, it will be required that the asset is retired. However, the retirement of the asset needs to be supported by a fully documented plan to migrate to a replacement asset that can take over the management of the process. The actual details of the plan will vary depending on the nature of the asset, but several core factors are required to be part of each migration plan:

- The name of the asset being retired, and the name of the asset being used for replacement.
- The date the migration will occur.
- The date the older system will be completely taken offline.
- A completed risk analysis that includes remediation plans for any identified high risks. (See Information Security Risk Management procedure.)
- Documented approval from the Change Advisory Board (see Change Management procedure).
- If applicable, the required data that needs to be backed up.
- A fallback plan should issues arise that prevents the replacement asset from being brought online.

Third Party Requirements:

For third party relationships that require the third party to have possession of an accountable technology asset, the contract with the third party will specify the return of all accountable technology assets upon termination of the contract. If the third party cannot return the technology asset, then they will be responsible for properly safeguarding and destroying the technology asset. Documentation containing the same information as Cone Health's Certificate of Destruction-Sanitization will be required from the third party after the technology asset is destroyed. Third party contracts will also impose limitations for use and disclosure of the information on a technology asset that cannot be returned.

Destruction/Sanitization by Shredding Services:
Contracts with shredding services will specify the following:

- Destruction method(s) used.
- Safeguards in place to prevent unauthorized access to technology assets awaiting destruction and in transit to a destruction facility.
- Protection of Cone Health from damages due to loss, theft, or unauthorized disclosure due to the fault of the vendor.
- Liability insurance requirements.
- Requirements for providing proof of destruction/sanitization in a timely manner to Cone Health.

Storage and Transportation of Technology Assets:
Physical storage and/or transportation of technology assets awaiting sanitization or destruction will be done in a manner that prevents unauthorized access and preserves chain-of-custody.

Business Machines/Medical Device Assets:
Hard drives for business machines and medical device assets will be sanitized or destroyed by Cone Health. If the asset is leased property, the lending organization will be contractually obligated to sanitize or destroy the hard drive. Lending agencies will provide Cone Health with documentation stating that they properly sanitized or destroyed the asset's hard drive.

Documentation Retention:
Records of maintenance and destruction/sanitization documentation will be retained for no less than 6 years from the date of the documentation.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.