Technology Equipment Disposal Policy

1.0 Purpose

Organizational technology equipment often contains sensitive data and components requiring special handling at the end of its lifecycle. Improper disposal poses significant risks, including data breaches if storage media are not securely sanitized, environmental harm, and potential legal non-compliance. Simply deleting files or formatting storage devices is insufficient, as data often remains recoverable. The purpose of this policy is to define the mandatory procedures for the disposal of all organizational technology equipment and components, ensuring secure data sanitization, environmentally responsible disposal, and proper asset management.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and affiliates of the organization. It covers any organization-owned or leased technology equipment or peripheral device that is no longer needed or has reached the end of its useful life. This includes, but is not limited to: personal computers (desktops, laptops, tablets), servers, mainframes, hard drives (internal/external), solid-state drives (SSDs), smartphones, handheld devices, peripherals (keyboards, mice, monitors, speakers), printers, scanners, copiers, fax machines, network equipment (routers, switches, firewalls, access points), removable storage media (USB drives, CDs, DVDs, floppy disks), backup tapes, batteries, and related printed materials containing sensitive information.

3.0 Policy Statements

3.1 Centralized Disposal Process

* **Mandatory Handover:** When organizational technology assets reach the end of their useful life or are no longer needed, they **must** be transferred to the designated organizational team responsible for asset disposal (hereafter referred to as the "Disposal Team"). Users or departments must not dispose of equipment independently.
* **Prohibited Disposal Methods:** Disposing of organizational technology equipment via unauthorized methods such as general waste skips, dumps, landfill, or unauthorized third parties is strictly prohibited. Unauthorized sale or donation of equipment is also prohibited.
* **Secure Handling:** The Disposal Team will manage the secure storage, data sanitization, and final disposal or repurposing of all received equipment.

3.2 Mandatory Data Sanitization

*   **Requirement:** Before any equipment containing storage media (hard drives, SSDs, USB drives, memory cards, mobile device storage, tapes, etc.) is disposed of, repurposed, sold, donated, or leaves organizational control, all organizational data, licensed software, and sensitive information **must** be securely and permanently removed (sanitized).
*   **Sanitization Standards:** Data sanitization must be performed by the Disposal Team using methods that meet or exceed established industry standards (such as NIST SP 800-88 Guidelines for Media Sanitization or DoD 5220.22-M). Acceptable methods include:
    *   **Overwriting:** Using approved disk sanitizing software to overwrite every addressable sector on the media multiple times with specified patterns (e.g., zero-filled blocks, random patterns). Simple file deletion or standard OS formatting is **not** sufficient.
    *   **Degaussing:** Using a powerful magnetic field to destroy the magnetic domains on magnetic media like hard drives and tapes (not effective for SSDs or optical media).
    *   **Physical Destruction:** Rendering the storage media physically unreadable and data unrecoverable through methods like shredding, crushing, disintegration, or incineration. This is the required method for SSDs if overwriting is not feasible or verifiable, and for media that are non-functional or cannot be effectively overwritten (e.g., some mobile devices, CDs/DVDs).
*   **Verification and Logging:** The Disposal Team must verify the successful sanitization of storage media. A record must be maintained, potentially including a sticker or tag affixed to the equipment case, indicating the sanitization method used, the date performed, and the initials or ID of the technician responsible.
*   **Non-Functional Media:** Storage devices that are non-functional and cannot be reliably sanitized via overwriting or degaussing must have the physical storage component removed and physically destroyed.

3.3 Employee Purchase Program (Optional)

*   The organization may, at its discretion, make certain functional equipment that has been securely sanitized and reached the end of its organizational lifecycle available for purchase by employees.
*   **Process:** If implemented, this program must use a fair and transparent system (e.g., a lottery) to provide equal opportunity for purchase. Employees cannot directly purchase or reserve their previously assigned equipment.
*   **Pricing:** The designated Finance and IT departments will determine appropriate pricing for items offered.
*   **Condition:** All equipment is sold "as-is," final sale, with no warranty, support, or licensed software provided by the organization.
*   **Inventory Removal:** All purchased equipment must be formally removed from the organization's asset inventory system before leaving the premises.

3.4 Final Disposal/Donation

*   Equipment not sold through the employee purchase program (if applicable), deemed non-functional, or unsuitable for reuse will be disposed of or donated.
*   Disposal must be carried out in an environmentally responsible manner, adhering to all applicable local, state, and federal regulations (e.g., e-waste recycling laws).
*   The Disposal Team will utilize contracted, reputable vendors specializing in secure IT asset

disposition (ITAD) and certified e-waste recycling or donation.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit, Asset Management) will verify compliance with this policy through various methods, including audits of the disposal process, review of sanitization logs and vendor certifications, physical inventory checks, internal/external audits, and investigation of any potential data incidents related to improper disposal.

4.2 Exceptions

Any exception to the procedures outlined in this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security) and potentially Legal or Compliance departments, depending on the nature of the exception.

4.3 Enforcement

Failure to comply with this policy, particularly the requirements for centralized disposal and secure data sanitization, may result in disciplinary action, up to and including termination of employment or contract. Improper disposal may also lead to legal liability for the organization and individuals involved.

5.0 Definitions

* **Data Sanitization:** The process of irreversibly removing or destroying data stored on memory devices (hard drives, SSDs, tapes, mobile devices, etc.) to make it unrecoverable.
* **Overwriting:** A data sanitization method using software to write patterns of data (e.g., zeros, ones, random characters) onto storage media sectors.
* **Degaussing:** A data sanitization method using a powerful magnetic field to neutralize the magnetic charge on magnetic media (hard drives, tapes).
* **Physical Destruction:** A data sanitization method that physically damages the storage media beyond the possibility of data recovery (e.g., shredding, crushing, incineration).
* **Disposal Team:** The designated organizational department or group responsible for managing the collection, data sanitization, and final disposition of retired technology assets (e.g., IT Asset Management, Facilities).
* **Technology Equipment:** Includes computers, servers, storage devices, mobile devices, network gear, peripherals, and related items as detailed in the Scope section.

6.0 Related Policies

* Asset Management Policy
* Data Classification Policy
* Information Security Policy (Overall)
* Record Retention Schedule / Policy

* Physical Security Policy
* Change Management Policy (for decommissioning servers/systems)

Revision #2
Created 28 August 2024 16:58:56 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery