Cybersecurity Policy Templates

Technology Equipment Disposal Standard

(Last Updated April 2025)

Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by <Company Name>.

Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within <Company Name> including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials. All <Company Name> employees and affiliates must comply with this policy.

Safeguards

Technology Equipment Disposal

When Technology assets have reached the end of their useful life they should be sent to the <Equipment Disposal Team> office for proper disposal.

The <Equipment Disposal Team> will securely erase all storage mediums in accordance with current industry best practices.

All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around <Company Name>. These can be used to dispose of equipment. The <Equipment Disposal Team> will properly remove all data prior to final disposal.

All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

The <Equipment Disposal Team> will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Employee Purchase of Disposed Equipment

Equipment which is working, but reached the end of its useful life to <Company Name>, will be made available for purchase by employees.

A lottery system will be used to determine who has the opportunity to purchase available equipment.

All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.

Finance and Information Technology will determine an appropriate cost for each item.

All purchases are final. No warranty or support will be provided with any equipment sold.

Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information

Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

Prior to leaving <Company Name> premises, all equipment must be removed from the Information Technology inventory system.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.