Technology Equipment Disposal Policy

Disclaimer

Free Use Disclaimer: This policy was created by Riskigy and 4THBIN for the community. All or parts of this policy can be freely used for your organization. There is no approval required. If you would like a new policy or updated version of this policy, please email media@riskigy.team

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security

risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Summary

Electronic data is more prevalent in today's organizations than physical printed data. Warehouses worth of documents can now be stored on computer hard drives, handheld devices and storage cards smaller than a fingernail. The bulk of many strategic operations depend on this digital information and the safe handling thereof.

Much of electronic data may contain confidential information, examples of which include, but are not limited to, the following data types:

- Bank account or other financial information
- Social security numbers
- Customer data
- Health care records
- Medical records
- Proprietary data
- Organizational "trade secrets"
- Employee records

Data often has a longer lifespan than the devices on which it is stored (or the time these devices spend in an employee's possession). A critical security risk can occur if confidential information is not properly removed from these systems before reassignment or disposal. Therefore, it is necessary to establish proper guidelines for electronic data disposal when devices are retired from use or reassigned to other employees.

Simply deleting a file or the contents of a device does not always guarantee that the data is removed. In many cases the operating system does not actually purge the file but instead marks the space on which it resides as available for use for future files to be written. For example, free programs like Recuva and FreeUndelete can be found on the internet and will easily recover recently deleted files on Windows systems, rendering them vulnerable to unauthorized access.

There are only three ways to adequately dispose of confidential information:

1. Secure "clearing" deletion of the specific files. Protects confidentiality of information against an attack by replacing written data with random data. Clearing must not allow information to be retrieved by data, disk or file recovery utilities.
2. Secure "purge" erasure (sanitization) of the entire storage media (e.g. hard drive). Protects confidentiality of information against an attack through either degaussing or secure erase.
3. Physical "destruction" of the storage media with intent is to completely destroy the media.

Recommended sanitization techniques for specific types of media are outlined in of NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations.

Purpose

The purpose of this policy is to provide guidelines for the appropriate disposal of information and the destruction of electronic media, which is defined as any storage device used to hold company information including, but not limited to, hard disks, magnetic tapes, compact discs, audio or video tapes and removable storage devices such as USB flash drives and micro-SD cards.

Electronic media may be designated for reuse, repair, replacement or removal from use in the ways described below.

This policy should be customized as needed to fit the needs of your organization.

Scope

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

All full-time employees, contract workers, consultants, part-time staff, temporary workers and other personnel are covered by this policy.

This policy applies to any device (whether employee or company-owned) which contains company data, including but not limited to computers, mobile devices, tablets and the storage media related thereto. It also applies to cloud provider environments. No applicable device shall change hands or be retired from use without being subjected to these guidelines. The only permitted exception to the "change hands" component is if the individuals involved already share the same data access (for instance one system administrator giving a computer to another system administrator). In this instance reformatting/reimaging the hard drive or resetting the device to factory defaults is considered acceptable.

Exceptions

There are no exceptions to this policy except unless noted below.

Any exception to the policy must be approved by the <CompanyName> Infosec Team in advance.

Policy

Technology Equipment Disposal

When Technology assets have reached the end of their useful life and/or end of life established by manufacturer they should be sent to the <CompanyName> office for proper disposal.

The <CompanyName> 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.

No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around <CompanyName>. These can be used to dispose of equipment. The <CompanyName> 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.

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

Cloud Services

There is no assurance that files stored on cloud provider systems such as Google, Amazon or Microsoft can ever be truly and permanently deleted since these are hosted on systems outside of <CompanyName> control.

Cloud providers take backups of customer data so employees should always proceed with caution before keeping confidential information on cloud provider systems. If utilizing cloud storage for confidential information has been approved by the <CompanyName> Information Security department, best practices for erasing the files in question involve removing rights to the file(s) from any people with whom it has been shared, deleting the file, then emptying any Trash or Recycling Bin offered by the cloud provider to ensure as sufficiently as possible that the document is no longer available.

Compliance

The <CompanyName> Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Procedures

NIST 800-88 Rev 1 Guidelines for Media Sanitization - http://csrc.nist.gov/publications/PubsSPs.html

Definitions and Terms

<Insert>

Revision History

Date	Summary of Change	Approved By
January 2023	Initial Draft	Riskigy and 4THBIN

Free Use Disclaimer: This policy was created by Riskigy and 4THBIN for the community.