Disposal Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company Staff store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media are phased out, sensitive information on the old equipment and media must be properly erased or otherwise made unreadable.

# II. Purpose

ABC Company faces several risks related to the disposal of hard drives and other computer storage media:

* Violation of Software License Agreements - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Usually these licenses are not transferable. Even when the licenses are transferable, there may be specific requirements that must be met, such as possession of the original distribution media, consent of the licensor, or payment of a transfer fee, in order to affect the transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims for damages.
* Unauthorized Release of Confidential Information - Allowing an unauthorized person access to confidential information can subject ABC Company and sometimes individual employees, to claims for damages.
* Unauthorized Disclosure of Trade Secrets, Copyrights, and Other Intellectual Property – ABC Company computer systems develop and store data, programs, designs, techniques, etc., that are or will become valuable assets of the organization as either trade secrets, copyrighted materials, patented inventions, or other intellectual property. Accidental or premature disclosure could mean a loss of secrecy under trade secrets law or constitute a publication under federal copyright law, either of which might result in loss of the asset.

# III. Scope

This policy applies to all ABC Company Staff that have access to Information Resources.

# IV. Policy

The Chief Security Officer shall ensure:

* Procedures address the final disposition of sensitive information, hardware, or electronic media.
* Procedures specify the process for making sensitive information unusable and inaccessible. Procedures specify the use of a technology (e.g. software, special hardware, etc.) to make sensitive information unusable, inaccessible, and not able to be reconstructed.
* Procedures specify the personnel authorized to dispose of sensitive information or equipment containing sensitive information. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed.

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled. Data can be present on any type of storage device, whether fixed or removable, that contains data and maintains the data after power is removed from the device. Due to the advances in computer forensics, simply deleting the data and formatting the disk will not prevent someone from restoring the data. However, sanitization of the storage media removes the information from the media in such a way that data recovery using common techniques or analysis is prevented.

Any and all computer desktops, laptops, hard drives, and portable media must be given to the IT Department for proper disposal. Paper and hard copy records should be disposed of in a secure manner as authorized by the Chief Security Officer (CSO). The CSO’s analysis of secure disposal processes should include, but not be limited to, shredders and storage of records in a secure area for an authorized disposal/recycling service.

Overwriting is a software procedure that replaces the data previously stored on magnetic storage media with a predefined set of meaningless data. At a minimum, overwriting should be performed using a character, its complement, then a random character. For confidential information, additional overwriting using different characters is recommended.

Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process.

Unless IT Department Staff can absolutely verify that no personal or confidential information, intellectual property, or licensed software is stored on the hard drive/storage media, the hard drive/storage media shall be sanitized or be removed and physically destroyed.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 5

HIPAA 164.310(d)(2)(i), 164.316(b)(2)(i)

ISO 27001 A.8.3.2

NIST SP 800-37 3.2, 3.7

NIST SP 800-53 MP-6, SA-19(3)

NIST Cybersecurity Framework ID.AM-2, ID.AM-3, ID.GV-3, PR.DS-3, DE.DP-2

PCI 3.1, 3.2