|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information and Media Disposal Policy | | | | | |
| Policy # | CPL-05-05 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc352611456)

[Scope 1](#_Toc352611457)

[Policy 1](#_Toc352611458)

[Information Disposal Standards 1](#_Toc352611459)

[Roles and Responsibilities 2](#_Toc352611460)

[Disposal of Hardcopy Records 2](#_Toc352611461)

[Litigation Hold 2](#_Toc352611462)

[Disposal of Electronic Media 2](#_Toc352611463)

[Disposal of Computer Equipment 3](#_Toc352611464)

[Transfer of Hard Drives and Media 3](#_Toc352611465)

[Violations 3](#_Toc352611466)

[Definitions 4](#_Toc352611467)

[References 4](#_Toc352611468)

[Related Documents 4](#_Toc352611469)

[Approval and Ownership 4](#_Toc352611470)

[Revision History 5](#_Toc352611471)

Purpose

This policy defines controls for the proper disposal of all Company X sensitive information, either in paper or electronic format.

Scope

This policy applies to all Company X computer systems and facilities, including those managed for Company X customers. This policy applies to all employees, partners and third-parties with access to Company X information assets in digital or hardcopy form.

Policy

### Information Disposal Standards

**Data Sanitization Standards** – The Information Security group is responsible for establishing standards for the proper sanitization of all computer equipment and media storage scheduled for destruction. These same standards must be used by any third-party vendor contracted to dispose of Company X equipment.

**Approved Disposal Vendor List** – Company X will maintain a list of commercial data disposal vendors that have been approved and certified by the Information Security Department to properly dispose of electronic media.

**Approved Software Vendor List** – Company X will maintain a list of approved commercial software packages and vendors which perform data overwriting operations. Company X personnel must only used approved software to overwrite electronic media.

### Disposal of Hardcopy Records

**Hardcopy Disposal** - When disposed of, all secret, confidential, or private information in hardcopy form must be either shredded or incinerated. To ensure that documents are properly destroyed, only shredders approved by Company X will be used to shred hardcopy records containing sensitive information.

**Secure Information Containers** – Sensitive information that is no longer needed must be placed in a designated locked destruction container within Company X offices and never placed in trash bins, recycle bins, or other publicly-accessible locations.

**Physically Securing Trash Dumpsters** - Company X trash dumpsters located outside Company X office buildings must be kept in a locked metal cage, and must be opened only for authorized trash hauling company staff.

### Litigation Hold

**Destroying Documents Relevant To Litigation** - If there is credible reason to believe that certain Company X internal documents may be needed as evidence in upcoming litigation, these documents must not be destroyed by the ongoing Company X document destruction process. They must instead be brought to the attention of internal legal counsel and then properly secured.

### Disposal of Electronic Media

**Storage Media Destruction** - Destruction of sensitive information captured on computer storage media must only be performed with approved destruction methods including shredders or other equipment approved by the Information Security Department.

**Disposal of Electronic Media Outside of Company X** - All electronic media other than computer hard drives must be erased, degaussed, or rendered unusable before leaving Company X. Employees must only use approved commercial vendors from the Disposal Approved Vendor List.

**Disposal of Media Containing Secret Data** – Company X must not resell or recycle media that contained highly classified data such as Trade Secrets. Media containing Trade Secrets must be sanitized and physically destroyed.

### Disposal of Computer Equipment

**Used Component Equipment Release** - Before disposal, donation, or recycling, the Information Security Department must validate that sensitive information has been removed from any information systems equipment that has been used for Company X business. This validation process must take place before releasing such equipment to a third party.

**Information And Equipment Disposal** - Department managers are responsible for the disposal of surplus property no longer needed for business activities in accordance with procedures established by the Information Security Department, including the irreversible removal of sensitive information and licensed software.

**Inventory Of Decommissioned Computer And Network Equipment** - The Information Security Department must maintain an inventory of all Company X computer and network equipment that has been taken out of commission. This inventory must also reflect all actions taken to clear memory chips, hard drives, and other storage locations in this same equipment of all stored information..

**Labeling Required** - Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly sanitized.

### Transfer of Hard Drives and Media

**Transfer of Hard Drives** - Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access the data by ordinary means. All electronic media should be sanitized according to Company X procedures.

**Transfer of Electronic Media** - Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

**Attempted Recovery** – Attempts to recover deleted or sanitized data must only be done by specially trained personnel approved by Company X management. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the Company X Confidentiality Statement.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

Confidential Information (Sensitive Information) – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement

Mobile Computing Devices - Mobile computing assets include, but are not limited to: laptop, notebook, tablet, desktop computers, all personal wireless-enabled devices, including pagers, cellular phones, mobile email devices, PDAs and other hybrid devices, and all portable storage media, including flash drives, smart cards, tokens, etc.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

Partner – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 4.7. Asset Disposal

PCI-DSS: PCI: 9.8 Media Destruction

HIPAA: Device and Media - Disposal (R)

ISO/IEC 27002 – 10.7.2 Disposal of media

NIST 800-53: MP-6 Media Sanitization

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |