|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Asset Management Policy | | | | | |
| Policy # | CPL-04-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

**Table of Contents**

[Purpose 1](#_Toc457886753)

[Scope 1](#_Toc457886754)

[Policy 1](#_Toc457886755)

[Asset Procurement 1](#_Toc457886756)

[Asset Inventory 2](#_Toc457886757)

[Ownership and Classification 2](#_Toc457886758)

[Equipment Authorization 2](#_Toc457886759)

[Property Removal 2](#_Toc457886760)

[Disposal of Computer Equipment 3](#_Toc457886761)

[Violations 3](#_Toc457886762)

[Definitions 4](#_Toc457886763)

[References 4](#_Toc457886764)

[Related Documents 4](#_Toc457886765)

[Approval and Ownership 4](#_Toc457886766)

[Revision History 4](#_Toc457886767)

Purpose

This policy establishes the minimum requirements and responsibilities for the protection of Company X equipment and media assets throughout the asset lifecycle.

Scope

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

Policy

### Asset Procurement

**Hardware And Software Procurement** - All hardware and software must be procured through the Purchasing Department according to company IT compatibility standards.

**Vendors Providing Mission Critical Hardware, Software, and Services** - All Company X mission critical hardware, software and services must be purchased, rented, leased, or otherwise obtained from a trusted and well-established vendor who is able to provide both maintenance services as well as warranties.

### Asset Inventory

**Asset Inventory - Technology** - The Information Systems Department must prepare an annual inventory of production information systems detailing all existing production hardware, software, and communications links.

**Asset Inventory - Information** - The Information Systems Department must compile and annually update a corporate-wide data dictionary and other high-level descriptions of the major Company X information assets.

**Asset Inventory Contents** – Every asset recorded in the Asset inventory must include the following information:

* Asset Name
* Asset Owner
* Asset Location
* Security Classification

**Equipment Tags** - All computer and communications equipment must have a unique computer-readable identifier attached to it such that physical inventories can be efficiently and regularly conducted.

**Controlling Inventory**- Company X Equipment Custodians must maintain perpetual inventory control, a record of the new location and new Equipment Custodian of all equipment issued to others, and physical security over the equipment in their possession.

### Ownership and Classification

**Asset Ownership** - All production information assets possessed by or used by Company X must have a designated owner with ownership responsibilities clearly documented.

**Security Classification** - Every Company X asset must be assigned a security classification.

**Responsibility Assignment** – Company X management must specifically assign responsibility for the control measures protecting every major information asset.

### Equipment Authorization

**Only Company Owned Devices** - Employees must not use personal computing devices to store or process Company X information. All mobile devices used for Company X business purposes must be issued by the Information Technology department.

**Approved Security Configuration** – All computer and communication equipment issued to users, including personal computers, mobile devices, and smart phones, must be configured according to standards approved by the Information Security Department.

### Property Removal

**Property Passes** - Information systems or business system equipment (desktop computers, modems, routers, etc.) must not leave Company X premises unless accompanied by an approved property pass.

**Media Removal** - All computer storage media containing sensitive information and leaving Company X offices must be accompanied by a properly authorized pass and must be logged at the building’s front desk.

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

**Approval For 3rd Party Removal** - Before Company X equipment of any type is sold, disposed of, recycled, donated, or otherwise conveyed to a third party, the written approval of the Information Security Department must first be obtained.

**Mobile devices must be returned for decommission** - All Company X issued mobile devices, including laptops, PDAs or cell phones must be returned to Company X when no longer in use by employees or contractors.

### ****Disposal of Computer Equipment****

**Information Systems Equipment Disposal** - 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.

**Outsourced data destruction must used approved methods** - Company X must verify the data specific methods of all third parties contracted for destruction of equipment containing sensitive data.

**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.

**FAX Machines Require Proper Disposal** - All Company X fax machines must have their internal disk drives properly erased before disposal or replacement according to sensitive information destruction procedures established by the Information Security Department.

**Devices Holding Secret Data Must Not be Resold** - Company X storage devices such as hard-drives, PDA’s, electronic cameras and cell phones which store Secret data must not be resold or recycled.  These devices must be destroyed using sensitive information destruction procedures established by the Information Security Department.

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.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

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.

**Information Asset –** Any Company X data in any form, and the equipment used to manage, process, or store Company X data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Third Party (Partner) –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**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.

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

References

CPL: 04.01 Asset Management

ISO/IEC 27002: 8.1 Responsibility for Assets

HIPAA: Device and Media - Accountability (A)

PCI-DSS: 9.5 Physically Secure Media

NIST: Media Protection (MP)

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 |  |
|  |  |  |  |  |