**POLICY APPROVAL**

|  |  |
| --- | --- |
| Approved By: |  |
| Approved Date: |  |
| Effective Date: |  |
| IT Governance Committee: |  |
| Board of Directors: |  |

**PURPOSE**

The purpose of this policy is to ensure that an asset management program is maintained to ensure proper control, management, assessment and planning regarding information technology assets at CompanyName.

No information technology asset may be placed in service in the company network/infrastructure without being inventoried. Inventory records of an asset must be maintained so long as CompanyName continues to own or lease the asset.

**SCOPE**

The scope of this policy includes all information technology assets owned or leased by CompanyName. Assets must be properly tracked from acquisition through useful service lifetime to the point at which each asset is disposed of – either through sale, gift or destruction.

This policy applies to all computers, laptops, servers, firewalls, routers, printers, faxes, scanners, credit card readers, swipe devices, other hardware devices and any other information technology asset that is either directly or indirectly connected to the company network (e.g., a dedicated printer connected to a computer).

Additionally, information technology assets temporarily or permanently removed from service are included in the inventory. A log of information technology assets disposed of will be kept for a minimum of 1 year from the disposal date.

**POLICY**

* An Approved Product List must be maintained containing information technology assets that can be purchased or leased for use on the network and by staff
* Newly acquired assets must be inventoried before they are placed into service on the company network/infrastructure
* Only IT staff may move, connect or disconnect information technology assets with the exception of explicit authorizations to IT staff for troubleshooting purposes
* Periodic inventories at a minimum on an annual basis of assets are conducted to ensure that all assets are accounted for, installed in their designated location and that no unknown assets are detected
* As required by PCI, assets supporting credit card transaction processing are labeled to indicate: owner, contact information and purpose unless deemed out-of-scope either due to meeting PCI point-to-point encryption requirements or a component of an off-network processing solution (i.e., completely independent from the company network)
* As required by HIPAA, assets that handle Electronic Protected Health Information (ePHI) must be identified as such along with physical location in the asset inventory
* Any “rogue” or unanticipated assets found during inventory will immediately be taken out of service and result in a security incident report and, as appropriate, quarantined, scanned, and an investigation involving the company, police and legal
* Any missing or unaccounted-for assets will result in a security incident report and may involve the company, police and legal if a suspected/actual theft has occurred
* Results of the periodic asset inventories are documented and made available as input to depreciation schedules, obsolesce planning and IT/general budgeting initiatives
* All information technology asset acquisitions must follow a formal process that involves appropriate IT staff in the decision-making process. If none of the assets on the approved products list meet the criteria the asset (make/model) must be added to the list before funds are committed to its purchase

**RESPONSIBILITIES**

| **Role** | **Responsibility** |
| --- | --- |
| Staff | Follow the formal request process for information technology asset requests. Do not move or connect/disconnect information technology assets unless explicitly authorized to do so by IT staff for troubleshooting purposes. |
| IT Staff | Ensure that the results of IT asset inventories are accounted for in: depreciation schedules, obsolesce planning and IT/general budgeting initiatives. |
| Information Security Officer | Ensure that up-to-date asset inventories are maintained; periodic asset inventories are conducted, and manage security incident activities related to information technology assets as appropriate. |

**REFERENCES**

|  |  |
| --- | --- |
| **Frameworks** |  |
| **Regulations and Requirements** |  |
| **Supporting Standards and Procedures** |  |

**REVISION HISTORY**

This section contains comments on any revisions that were made to this document and the date they were made.

| **Revision Number** | **Date** | **Name** | **Description** |
| --- | --- | --- | --- |
| 1.0 | DateV |  | Initial Version |