Asset Inventory – Policy and Procedure

Version: 1.0

Date:

Goal:

To maintain an inventory of current assets so that an appropriate level of protection of organization assets can be achieved. This is done through asset documentation, ownership, and risk rankings.

Scope:

[Company name] must maintain inventories of all important information assets. The scope of this policy is inclusive of all IT assets that are owned or hosted by [Company name], is hosted on behalf of [Company name] by a cloud vendor or is located at a shared date center facility. At this time the current scope for maintaining inventory on assets includes:

- End user compute devices (computers, laptops)
- End user applications
- Cloud based (SaaS) applications
- Company provided endpoints for employees
- Company provided endpoints for contractors and/or consultants
- Employee owned (BYOD) endpoints used on premises.
- Company owned servers onsite
- Non-company owned servers onsite
- Company owned servers at vendor or partner locations
- Non-company owned servers located at vendor or partner locations
- IoT devices on company premises like HVAC and alarm systems.
- Company owned servers at offsite data center.
- Company owned networking infrastructure onsite
- Company owned access badges
- Company owned mobile devices
- Company access devices (keys to building / elevators)

(Cross off or delete any assets you do not want to include in the scope of your inventory management at this time.)

Required fields:

Data required to be collected and retained as part of the asset inventory process is:

- Asset name (DNS, hostname, Application name)
- Approval (Checkbox field that the asset has been verified as appropriate to the environment)
- Device Type (computer, server, laptop, end user application, cloud application)
- Description (field to provide basic description)
- Asset Location (on prem, mobile, cloud)
- IP Address (any protocol assignment associated with asset, can be IP range)
- Asset Owner (group that owns, maintains, or requires this asset)
- Risk Classification (unknown, low, medium, high)
- Risk Assessment Performed (NA, none, or date)
- Notes

Inventory System:

The assets shall be inventoried in a central repository. This source should be independent and regarded as the authoritative source of trust for the inventory is maintains. Procedures will exist to reconcile and update this inventory. No automated processes should update this inventory from a subjective inventory, such as other security management console.

Asset Owners:

All information assets must have owners, within the context of the organization. Assets owner is responsible for the providing risk classification information consistent with data classification policy levels. If the ownership for a specific type of asset has not yet been clearly assigned to a specific owners, it will be temporarily default to the [role name].

Asset Monitoring:

Assets should be continuously monitored, as part of the cybersecurity vulnerability management program.

Asset Inventory: Management Process

Inputs:

Assets will be discovered and ingested from other appropriate technology tools and resources. Data exports, or manual exports can be performed to populate the inventory asset list.

For example, for cloud applications (SaaS) can be exported from [system name]. Endpoint resources can be exported from [system name].

Review:

Assets will be reviewed with the asset owner for appropriateness within the environment. Once a single approval is achieved the asset is approved unless the data owner provides written notice the asset is no longer approved.

Discovery:

Ongoing processes will be used detect new, rouge, or malicious assets introduced in the environment.

- Utilize Discovery Tools: Utilize active and passive discovery tools such as scanners, Active Directory, and other resources to discover new assets.
- Log Sources: Log sources can be used and reviewed to identify previously unknown assets such as DHCP, and DNS logs.

Reconcile:

Assets identified as part of the discovery process will be reconciled against the source of truth asset inventory list. Assets identified, that were not currently previously in the asset list, will be reviewed for ownership assignment and approval by ownership to be included in the asset inventory list.

Maintain:

An ongoing governance task will be created and assigned to regularly review the asset inventory list. This maintain process will ensure the following:

- Discovered assets are being added
- Asset ownership and fields are being updated
- Information is accurate and up to date