# ASSET MANAGEMENT POLICY

For this policy, the following stakeholders may be involved with data gathering and review:

* IT
* Security
* Legal and Privacy
* Data Manager (as applicable)
* Procurement
* Code / Software Development

What is the name of your company? (Replaces all the “Company” options)

|  |  |  |  |
| --- | --- | --- | --- |
| Version: | **{{version}}** | Effective Date: | {{effective\_date}} |
| Owner and Title: | {{owner\_title}} | **Approver and Title:** | What is the name and title of the individual -typically, an executive - who approves this policy? |
| Last Review Date: | When was the last review date of this document? (If new document, enter N/A) | **Next Review Date:** | What is the next review date of this document? (Typically, a year after creation/last date) |

**Applicability**

This Policy applies to all Company employees, directors, and officers; any other individual or organization performing work for Company, including those employed by third parties, (collectively known as “Users”), all data and systems, including those employed by third parties, (collectively known as “Assets”); and business processes used by or supporting Company.

**Scope**

What is the physical scope of the policy? Choose from the drop-down options or enter custom answer)

Lucas – see options in the “Choose an item” drop down hereChoose an item.

**Target Audience**

What type of users does policy apply to? Choose from the drop-down options or enter custom answer)

Lucas – see options in the “Choose an item” drop down hereChoose an item.

**Purpose**

The Asset Management Policy outlines Company approved requirements for identifying, protecting, and managing assets (software, hardware, and data) through the asset lifecycle, from initiation/procurement, configuration, deployment, use of, disposal to avoid data loss, asset destruction, unintended manipulation, or other threat.

This Policy details Company’s requirements for:

* Facilitating a consistent approach to identify, classify and handle assets across the organization throughout the asset lifecycle.
* Protecting Company What are your sensitive assets classified as? Typically, they are labeled with Confidential, Sensitive, Internal Use Only assets from unauthorized use, access, distribution, alteration, and deletion / disposal.
* Assigning the appropriate level of security controls to safeguard Company assets by their classification.
* Handling of Company assets when no longer required for business purposes.
* Requiring the secure disposal and preparation for the reuse of Company assets.
* Ensuring Company compliance with applicable laws and regulations, to include. Which laws and regulations are applicable to your organization? If none, leave blank. If blank, remove the two words “to include”

# Key Points to Remember

* The term “assets” used is applicable to hardware, software, and data.
* Assets are given a classification which demonstrates how critical and/or sensitive they are.
* Assets are to be safeguarded with controls that align with the designated classification.
* The higher the asset’s classification, the more stringent the security controls for the asset.
* Assets are to be protected, per their classification, through each stage of the lifecycle (initiation/procurement, configuration, deployment, use of, disposal/ destruction).

**Policy Compliance**

This Policy shall take effect upon publication. Defined users of Company’s assets Select one: must, shall, will, should, may comply with the requirements outlined in this Policy.

Is there other legal content you would like to include? If none, leave blank.

**Policy Violation**

The Policy Owner Select one: must, shall, will, should, may be notified of material breaches of this Policy, whether intentional or inadvertent. Violation of these Policies Select one: must, shall, will, should, may be subject to disciplinary action, up to and including termination. Company retains discretion as to how to respond to violation of this Policy and shall undertake disciplinary process in accordance with all applicable laws and other legal requirements.

Is there other legal content you would like to include? If none, leave blank.

**Policy Exceptions**

Company Select one: must, shall, will, should, may grant exceptions to this Policy subject to written approval from the Company Who is the title who may approve exceptions? Exceptions granted Select one: must, shall, will, should, may not undermine the requirements set forth in this Policy.

Exception requests Select one: must, shall, will, should, may be submitted in writing to the Company Who is the title who may approve exceptions? with justification for the requested exception. Exception requests Select one: must, shall, will, should, may include potential risks of the exception and compensating controls to address residual risk.

Granted exceptions Select one: must, shall, will, should, may be documented and retained for the life of the exception. Exceptions Select one: must, shall, will, should, may be subject to review on a How frequently are granted exceptions reviewed? basis and potentially reassessed to ensure risk is not introduced to Company.

**Supplemental Information**

List documents and their location for relevant information If they have none, can be N/A. If more than one, can more lines be added?

Name of document Link or location

**Controls Alignment**

* **NIST CSF 2.0:** ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08
* **CIS Critical Security Controls:** 1.1, 2.1, 3.2, 3.5, 3.7, 3.8

**POLICY**

1. **Asset Management**

**1.1 Scope**

Physical assets include hardware, mobile devices, or supporting infrastructure involved in the processing, transport, storage, usage of Company data and/or otherwise involved in Company business processes.

Software assets include software, applications developed in-house or by a third-party, or supporting software infrastructure involved in the processing, transport, storage, usage of Company data and/or otherwise involved in Company business processes.

Data assets include data created or owned by Company, whether handled by Company users or third parties on behalf of Company.

The scope includes third parties when using Company assets, their own assets in support of Company, and/or are connected to Company’s environment.

**1.2 Asset Discovery**

Scans Select one: must, shall, will, should, may be performed How frequently are scans performed to identify assets? to identify internal and external physical and software assets connected to Company’s network. Detected unauthorized assets Select one: must, shall, will, should, may be addressed and Select one: must, shall, will, should, may be tracked with Company’s risk management processes.

Scans Select one: must, shall, will, should, may be performed How frequently are scans performed to identify data assets? to identify data present in Company’s environment.

Controls to identify sensitive data when improperly stored and transmitted through and outside Company’s environment Select one: must, shall, will, should, may be in place and set to block and notify the Which group/s should be notified when sensitive data being insecurely handled? to research further.

**1.3 Asset Classification**

Company assets Select one: must, shall, will, should, may be assigned a classification and handled as defined in the CompanyAssetClassification and Handling Policy, to ensure adequate protection and efficient utilization through their lifecycle.

**1.4 Asset Inventory**

An inventory of enterprise assets Select one: must, shall, will, should, may be maintained and an owner Select one: must, shall, will, should, may be designated to each asset. Assets Select one: must, shall, will, should, may be classified per the Company Asset Classification and Handling Policy, uniquely identified, and assigned an asset owner classification.

Organizational communication and data flows Select one: must, shall, will, should, may be mapped to ensure understanding of asset purpose and usage in the Company environment.

Asset inventories Select one: must, shall, will, should, may be reviewed How frequently should asset inventories be reviewed for accuracy? to ensure accuracy, completeness, and reduce unintentional duplication of information. Updates Select one: must, shall, will, should, may be performed at the time of the inventory review.

Integrity checking mechanisms Select one: must, shall, will, should, may be used to verify the integrity of software, firmware, and hardware.

**1.5 Asset Lifecycle Management**

Company assets Select one: must, shall, will, should, may effectively managed through their lifecycles, from procurement / creation through configuration to deployment to deletion / disposal.

**Asset Acquisitions**

Physical and software assets Select one: must, shall, will, should, may be procured from verified and reputable vendors. Prior written approval Select one: must, shall, will, should, may be obtained from What are the group/s prior written approval is obtained?.

Assets Select one: must, shall, will, should, may be configured and aligned with Company security standards and evaluated for potential security risks prior to deployment.

Unauthorized software programs Select one: must, shall, will, should, may downloaded and used.

Software installation policies Select one: must, shall, will, should, maybe enforced.

**Asset Deployments**

Physical and software assets Select one: must, shall, will, should, may be configured and deployed following Company standards, procedures, and requirements.

A security configuration review Select one: must, shall, will, should, may be conducted and necessary security tools Select one: must, shall, will, should, may be installed prior to implementation.

Software installations Select one: must, shall, will, should, may be recorded and comply with licensing agreements.

**Asset Protection**

Physical assets Select one: must, shall, will, should, maybe minimally safeguarded per their defined classification in the Company Asset Classification and Handling Policy.

Software assets Select one: must, shall, will, should, maybe minimally safeguarded per their defined classification in the Company Asset Classification and Handling Policy.

Data assets Select one: must, shall, will, should, maybe minimally safeguarded per their defined classification in the Company Asset Classification and Handling Policy.

**Asset Maintenance and Management**

Physical and software assets Select one: must, shall, will, should, maybe kept updated and current with Company requirements for patch management and system/firmware upgrades.

Assets Select one: must, shall, will, should, may be monitored for performance and security status.

Data in production environments Select one: must, shall, will, should, maybe kept separate from other business environments, and Select one: must not, shall not, will not, should not, may not be used for development and testing purposes.

Periodic risk assessments Select one: must, shall, will, should, may be performed.

**Asset Reuse**

Assets, whether managed by Company or by a third party, Select one: must, shall, will, should, may be sanitized or securely erased to ensure there is no residual data.

Assets being reused Select one: must, shall, will, should, may be tested to ensure there is no residual data prior to being provided to another user or put to other use.

Records Select one: must, shall, will, should, may be maintained to document actions taken to securely delete data and prepare for asset reuse.

**Asset Deletion / Disposal**

Data no longer required for business use Select one: must, shall, will, should, maybe disposed of or sanitized securely and in compliance with Company -approved methodologies.

Systems with Company data managed by a third party Select one: must, shall, will, should, may be disposed of or sanitized, according to its classification defined in the Company Asset Handing and Classification Policy.

AssetSelect one: must, shall, will, should, maybe removed from the asset inventory.

Disposal documentation Select one: must, shall, will, should, maybe maintained for audit purposes.

**Review**

This Policy Select one: must, shall, will, should, may be reviewed periodically (at least How often should this policy be reviewed? It is typically annually) and/or after any significant changes to Company’s business practices or processing environment(s), to ensure that the contents remain current and appropriate.

New revisions of the Policy Select one: must, shall, will, should, may be published.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Type | Date: | Change Details |
| 1.0 | Original Issue | What date should be used for policy creation? | No Change |
| 1.1 | Review | What date should be used for the next review date of the policy? | What changes were made in this update? If none, state N/A. |

**END OF POLICY**