Physical Devices Inventory (ID.AM-1)

POLICY # CS-2	EFFECTIVE DATE January 1, 2024	APPROVED BY Insert Approver
VERSION # 1.1	LAST REVISED Insert Last Revised Date	REFERENCE NIST CsF: Asset Management Physical Devices Inventory (ID.AM-1)

Purpose

To describe the activities required to perform an inventory of the organization's physical assets and systems.

Scope

This policy applies to all ORGANIZATION_NAME workforce members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, authorized third parties, and anyone else granted access to sensitive information by ORGANIZATION_NAME.

Policy

Physical devices and systems within the organization are inventoried.

- Develops and documents an inventory of physical devices and information system components that:
  - Accurately reflects the current information system.
  - Includes all components within the authorization boundary of the information system.
  - Includes information deemed necessary to achieve effective information system component accountability.
  - Reviews and updates the inventory of physical devices and information system component.
- ORGANIZATION_NAME develops and maintains an inventory of its information systems.

Inventory of Assets

- An inventory of assets and services will be maintained. ORGANIZATION_NAME's asset inventory will not duplicate other inventories unnecessarily and ORGANIZATION_NAME will ensure their respective content is aligned.
- The inventory of all authorized assets will include the owner of the information asset, custodianship, categorize the information asset according to criticality and information classification, and identify protection and sustainment requirements commensurate with the asset's categorization.
- ORGANIZATION_NAME will provide an updated inventory identifying assets with covered information (e.g., ePHI, PII) to the information security official, and the senior privacy official on an organization-defined basis, but no less than annually.

Responsibilities

The Information Security Officer is responsible for ensuring compliance with these polices. Additionally, all individuals, groups, and organizations identified herein are responsible for compliance with all NIST Cybersecurity Framework policies.

The ORGANIZATION_NAME Information Security Officer, is responsible for:

- The development, implementation, and maintenance of ORGANIZATION_NAME security policies.

- Working with employees to develop procedures and plans in support of security policies.

The Information Security Officer is responsible for conducting at least an annual review of the Physical Devices Inventory Policy, making any appropriate changes, and disseminating the updated policy to workforce members.

Retention

Every policy and procedure revision/replacement will be maintained for a minimum of six (6) years from the date of its creation or when it was last in effect, whichever is later. Other ORGANIZATION_NAME requirements may stipulate a longer retention. Log-in audit information and logs relevant to security incidents must be retained for six (6) years or a longer period, depending on the strictest regulatory mandate.

Compliance

This policy addresses the requirements of the Identify Function. Failure to comply with this or any other security policy will result in corrective actions as per the Disciplinary Process Policy. Legal actions also may be taken for violations of applicable regulations and standards such as NIST.

Related Form(s) and Evidence

- None

References

- NIST Cyber Security Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework v1.1 – Related Standards	
Standard	**Description**
FERPA	Inventory of assets: Include both authorized and unauthorized devices used in the computing environment
NIST SP 800-53 R5	CM-8 System Component Inventory PM-5 System Inventory
NIST SP 800-171 R2	3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
HIPAA Security Rule	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC 164.310(a)(2)(ii) Facility Security Plan (A) SPEC 164.310(d)(1) Device and Media Controls SPEC
ISO 27001:2022	A.5.9 Inventory of information and other associated assets
HITRUST v11.2.0	07.a Inventory of Assets

Contact

Insert Contact Person
Insert Full Address

E: Insert Email ID

P: Insert Phone No.

Policy History

Initial effective date: January 1, 2024.