Physical Devices Inventory (ID.AM-1)

Policy #: CS-2 **Approved by:** Uday Ali Pabrai, CEO

Version #: 1.1 **Effective Date:** August 1, 2019

Purpose
To describe the activities required to perform inventory of organizations 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.
- The 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
Compliance and review are the responsibility of the designated Information Security Officer.

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.

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

NIST Cybersecurity Framework v1.1 – Information Protection Program Policy-Related Standards	
Standard	**Description**
FERPA	Inventory of assets: Include both authorized and unauthorized devices used in the computing environment
NIST SP 800-53	CM-8: Information System Component Inventory PM-5: Information System Inventory
NIST SP 800-171r1	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	HIPAA § 164.308(a)(1)(ii)(A) HIPAA § 164.310(a)(2)(ii) HIPAA § 164.310(d)(1)
ISO 27001:2013	A.8.1.1: Inventory of assets A.8.1.2: Ownership of assets

Contact

Name (Information Security Officer)
1234 Anystreet
Anywhere, IL 55555

E: Insert Email
P: Insert Phone
F: Insert Fax

Policy History: Initial effective date: August 1, 2019