Asset Management Policy

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.5

Table 2: Document history

Date	Comment
Apr 21 2026	Initial document

1 Purpose and Scope

a. The purpose of this policy is to ensure that all information assets owned or managed by IronHub are identified, inventoried, assigned ownership, and protected in accordance with their classification and risk.

b. This policy applies to all hardware, software, data, cloud services, and other information assets that support IronHub's operations and information security program.

c. This policy applies to all employees, contractors, and vendors who acquire, manage, or use IronHub's information assets.

2 Background

a. Effective security begins with knowing what assets exist and who is responsible for them. An accurate and maintained asset inventory enables proper access controls, vulnerability management, and secure decommissioning.

3 Definitions

a. **Asset**: Any item of value to the organization, including hardware devices, software applications, cloud services, data repositories, and intellectual property.

b. **Asset Owner**: The individual or team responsible for a particular asset's security, maintenance, and lifecycle management.

c. **Asset Register**: The centralized inventory of all organizational assets.

4 Policy

4.1 Asset Inventory

a. IronHub must maintain a centralized Asset Register that includes all information assets. The register must be reviewed and updated at least **quarterly** and whenever assets are added, changed, or decommissioned.

b. The Asset Register must include, at minimum, for each asset:

   i. Asset name and description.

   ii. Asset type (hardware, software, cloud service, data repository, etc.).

   iii. Asset owner and custodian.

   iv. Location (physical or logical, e.g., AWS region, office location).

v. Data classification of the information the asset stores or processes (per the Data Classification Policy).

vi. Acquisition date and, where applicable, license expiry or renewal date.

vii. Decommission date (if applicable).

c. The ISM is responsible for maintaining the Asset Register and ensuring it remains accurate.

4.2 Asset Ownership

a. Every asset in the Asset Register must be assigned an **Asset Owner** responsible for:

i. Ensuring the asset is appropriately secured in accordance with its classification.

ii. Authorizing access to the asset.

iii. Participating in periodic access reviews.

iv. Managing the asset through its lifecycle including decommissioning.

b. Asset ownership must be reviewed and updated when personnel change roles or leave the organization.

4.3 Hardware Asset Management

a. All company-owned hardware (laptops, desktops, servers, mobile devices, network equipment) must be recorded in the Asset Register upon procurement.

b. Hardware assets must be assigned to a named user or team. Unassigned hardware must be stored securely.

c. Hardware that is lost or stolen must be reported to the ISM and IT immediately. The incident must be handled in accordance with the Security Incident Response Policy.

4.4 Software and Cloud Service Management

a. All software applications and cloud services used in production or with access to company data must be recorded in the Asset Register, including Software-as-a-Service (SaaS) tools.

b. Unauthorized or unapproved software and cloud services must not be used to store or process company data. Employees who discover unauthorized software or services in use must report it to the ISM.

c. Software licenses must be tracked and renewed before expiry.

4.5 Secure Disposal and Decommissioning (CC6.5)

a. Before any asset is decommissioned, retired, or transferred, all organizational data must be securely removed from the asset. Data removal methods must be appropriate for the data classification:

   i. **Confidential and Restricted data**: Cryptographic erasure or physical destruction of storage media.

   ii. **Internal Use data**: Secure wipe using NIST 800-88 guidelines or equivalent.

   iii. **Public data**: Standard deletion is acceptable.

b. Decommissioned hardware must be removed from the Asset Register and from all access control systems before disposal.

c. Disposal of hardware containing storage media must be documented, including the disposal method, date, and responsible party. Third-party disposal vendors must provide a certificate of destruction.

d. Cloud service decommissioning must include deletion of all data, revocation of API keys and credentials, and removal of integrations, confirmed in writing before the service contract is terminated.

4.6 Periodic Review

a. The Asset Register must be reviewed against actual deployed assets at least **annually** (or quarterly for critical assets) to identify undocumented assets, orphaned accounts, or assets no longer in use.

b. Assets discovered that are not in the Asset Register must be assessed for risk, assigned an owner, and added to the register promptly.

5 Enforcement

a. Asset owners are accountable for the security of their assigned assets. Failure to maintain accurate asset records or to follow secure disposal procedures may result in disciplinary action.

b. The ISM may audit asset inventories at any time to verify compliance with this policy.