Asset Management Policy

VERSION	EFFECTIVE DATE	POLICY OWNER
1.0	2026-07-31	Matt Sapio, CISO

APPROVED BY
Matt Sapio

1. Purpose

This policy establishes requirements for identifying, tracking, handling, protecting, and securely disposing of Eigenomic assets, including cloud, software, data, and endpoint assets. It is designed to protect company and customer information, support operational continuity, and support Eigenomic's SOC 2 security objectives.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who manage, maintain, or use assets owned, leased, or controlled by Eigenomic. As a fully remote, cloud-based organization with fewer than five employees, Eigenomic's assets primarily include AWS resources, software, accounts, data, intellectual property, and authorized endpoint devices.

3. Inventory of Assets

- **Asset Documentation:**
  - An inventory must be maintained for assets that are material to Eigenomic's operations or information security.
  - Asset records should identify the asset, responsible owner, relevant location or cloud environment, and current status, as applicable.
  - The inventory is updated regularly and reviewed periodically to ensure accuracy and completeness, addressing the requirements of SOC 2 and applicable legal,

contractual, and security requirements.

- **Asset and Information Classification:**
  - Assets that store, process, or provide access to sensitive or customer information must be identified and protected according to the sensitivity of the information.
  - Classification aids in applying appropriate handling and security controls.

4. Ownership of Assets

- **Designated Ownership:**
  - Every asset must have an assigned owner who is responsible for its lifecycle management, security, and integrity.
  - Asset owners define access levels, monitor usage, and ensure that handling procedures are followed.
  - Clear ownership supports accountability and is critical for timely incident response and risk mitigation.

5. Acceptable Use of Assets

- **Permitted Use:**
  - All users must utilize company assets only for approved business purposes.
  - Any personal use must be minimal and must not compromise operational security or compliance with applicable regulations.
  - Misuse or unauthorized actions are subject to disciplinary measures.

6. Loss or Theft of Assets

- **Incident Reporting:**
  - Any loss or theft of assets must be reported immediately to the IT or security department.
  - Reports should detail the last known location, circumstances, and any steps taken to mitigate potential risks.
  - The incident response team will assess the impact and implement protective measures, meeting the notification and mitigation requirements of SOC 2 and applicable legal, contractual, and security requirements.

7. Return of Assets

- **End-of-Employment or Contract:**
  - Upon termination or contract completion, all company assets—including hardware, software, and data—must be returned promptly.
  - The designated responsible role must document returned company assets and update applicable asset records.
  - This process helps prevent unauthorized retention of sensitive data and supports compliance with SOC 2 and applicable legal, contractual, and security requirements.

8. Handling of Assets

- **Secure Management:**
  - Physical endpoint assets must be reasonably secured against loss, theft, damage, or unauthorized access in remote work environments.
  - Digital assets must be protected in line with the organization's data protection standards, including the use of encryption, access controls, and regular security assessments.
  - Assets containing sensitive or customer information must be handled in accordance with applicable legal, contractual, and security requirements.

9. Asset Disposal and Reuse

- **Lifecycle Management:**
  - When an asset reaches the end of its useful life, it must be disposed of securely or reused following defined procedures.
  - Data sanitization techniques—such as secure wiping or physical destruction—must be applied to eliminate any residual sensitive information.
  - The disposal process is documented and verified to ensure adherence to legal and regulatory requirements.

10. Customer Asset Return

- **Customer-Owned Assets:**

- Assets owned by customers and held by the organization must be managed with heightened security and confidentiality.
- Upon service completion or customer request, assets are returned securely after verifying that no sensitive company or customer data remains.

11. Exceptions

- **Approved Deviations:**
  - Any exceptions to this policy require formal approval by the designated authority or relevant department.
  - Approved exceptions must be documented, including the risk assessment and any compensatory controls, and reviewed periodically to ensure ongoing compliance.

12. Violations and Enforcement

- **Enforcement Measures:**
  - Non-compliance with this policy may result in disciplinary actions, including termination or legal proceedings, depending on the severity of the violation.
  - The Policy Owner or designated responsible role monitors adherence and addresses identified violations.