Data Management Policy

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

APPROVED BY
Matt Sapio

1. Purpose

This policy establishes comprehensive guidelines for managing data throughout its lifecycle to ensure its confidentiality, integrity, and availability. It standardizes data handling practices across departments and supports compliance with industry and regulatory requirements, including SOC 2, ISO 27001:2022, applicable legal and contractual requirements, applicable contractual or security requirements 4.0, GDPR, and US Data Privacy.

2. Scope

This policy applies to all Eigenomic employees, contractors, systems, applications, AWS resources, and approved third-party services that create, access, process, transmit, store, or dispose of company or customer data, including data associated with custom automation software developed for law offices.

3. General Requirements

- **Commitment to Data Protection:**
  - The organization ensures that all data is managed in a manner that protects against unauthorized access, loss, or alteration.
  - Data handling practices are designed to meet both internal standards and external regulatory obligations.

4. Data Classification

Data is classified based on sensitivity, criticality, and regulatory obligations. The following classifications are defined:

- **Confidential:**
  - Data that demands the highest level of protection due to potential financial, legal, or reputational risks.
  - Access is strictly limited to authorized personnel.
- **Restricted:**
  - Sensitive data that requires controlled access, with sharing permitted only with trusted third parties under strict agreements.
- **Public:**
  - Data intended for open access. Even though this data is not sensitive, it must be periodically reviewed for accuracy and appropriateness.

5. Labeling

- **Consistent Identification:**
  - All data, whether physical or electronic, must be clearly labeled according to its classification.
  - Electronic data should include metadata tags, watermarks, or access control markers, while physical data must be securely labeled to prevent unauthorized handling.

6. Data Handling

- **Confidential Data Handling:**
  - Must be encrypted during both transmission and storage.
  - Access is restricted to designated personnel, and any physical copies are secured in controlled environments.
- **Restricted Data Handling:**
  - Encryption is required when transmitted externally, and data must be stored in environments with controlled access.

- Sharing is permitted only with approved third parties under strict security controls.

- **Public Data Handling:**
  - May be shared openly; however, its accuracy and relevance must be maintained to prevent misuse.

7. Data Retention

- **Retention Policies:**
  - Data is retained only as long as necessary to fulfill business, legal, and regulatory requirements.
  - Retention periods are defined according to data classification and are subject to periodic review.
- **Secure Archival and Disposal:**
  - Data that exceeds its retention period must be securely archived or disposed of according to established procedures.

8. Data & Device Disposal

- **Secure Destruction:**
  - Sensitive data must be rendered unrecoverable through secure deletion methods, such as certified data-wiping software or physical destruction for devices.
  - Hard copies of sensitive data should be shredded or incinerated following confidentiality guidelines.
  - All disposal activities must be documented to ensure compliance and accountability.

9. Annual Data Review

- **Ongoing Validation:**
  - An annual review is conducted to confirm the accuracy of data classification, assess compliance with retention schedules, and identify outdated or redundant information.
  - This review supports continuous improvement and adherence to regulatory requirements.

10. Legal and Regulatory Compliance

- **Adherence to Standards:**
  - Data management practices must comply with all applicable data protection and privacy regulations, including GDPR, applicable legal and contractual requirements, SOC 2, and applicable contractual or security requirements 4.0.
  - Regular audits are performed to verify compliance, and the policy is updated as necessary to reflect changes in regulatory requirements, including breach notification obligations and security control mandates.

11. Policy Compliance

- **Mandatory Adherence:**
  - All employees, contractors, and third-party service providers must comply with this policy.
  - Compliance is monitored through periodic audits and data management reviews.
  - Non-compliance may result in disciplinary actions, including termination or legal recourse.

12. Exceptions

- **Formal Approval Process:**
  - Exceptions to this policy may only be granted by the Policy Owner.
  - All exceptions must be documented, justified, and reviewed annually to ensure that alternative controls sufficiently mitigate any associated risks.

13. Violations and Enforcement

- **Enforcement Measures:**
  - Violations of this policy will result in disciplinary actions, which may include termination or legal action, depending on the severity and impact of the infraction.
  - Periodic audits and assessments are conducted to ensure adherence to this policy and to promptly address any violations.