# Cryptography 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 the implementation and management of cryptographic controls used to protect Eigenomic and customer information. It supports the confidentiality, integrity, and availability of data within Eigenomic's fully cloud-based AWS environment and supports SOC 2 security objectives.

## 2. Scope

This policy applies to all Eigenomic personnel and third parties who handle, store, transmit, or administer sensitive information or cryptographic controls. It applies to Eigenomic's AWS infrastructure, applications, endpoints, and approved third-party services.

## 3. General Requirements

### Encryption Standards

- **Data Protection:**
  - Sensitive and customer data must be encrypted in transit and at rest using approved, industry-standard cryptographic methods where technically applicable.
  - Encryption protocols must align with applicable legal, contractual, security, and SOC 2 requirements.

### Access Control and Authentication

- **Restricted Access:**
  - Only authorized personnel are permitted to access systems and applications that utilize cryptographic controls.
  - Access to encrypted data is managed through role-based access control (RBAC) and multi-factor authentication (MFA), preventing unauthorized decryption.

### Cryptographic Implementation

- **Algorithm Selection:**
  - Cryptographic solutions must use current, industry-accepted algorithms and protocols appropriate to the data and system risk.
  - Approved implementations should use strong, widely accepted cryptographic standards and avoid deprecated or known-weak algorithms.

## 4. Key Management

### Key Generation and Storage

- **Secure Generation:**
  - Cryptographic keys must be generated and protected using approved key-management capabilities, including AWS key-management services where applicable.
  - Keys are stored in secure environments to prevent unauthorized access and tampering, with all key usage logged and monitored for audit purposes.

### Key Rotation and Expiration

- **Scheduled Updates:**
  - Keys must be rotated or replaced based on system capabilities, risk, applicable standards, and defined key-management requirements.
  - Expired keys are securely destroyed and replaced without service disruption, ensuring continuous compliance with regulatory guidelines.

### Key Revocation and Destruction

- **Immediate Response:**

- In the event of an employee termination, a partner relationship ending, or a key compromise, affected keys must be revoked immediately.
- Revoked or expired keys are securely destroyed following established secure disposal procedures.

### Key Management Matrix

The following table outlines the required parameters for key management:

| Domain | Key Type | Algorithm | Key Length | Review / Rotation |
|---|---|---|---|---|
| Data Encryption | Symmetric | AES-256 | 256 bits | 2 years |
| Digital Signatures | Asymmetric | RSA-2048 | 2048 bits | 3 years |
| Communication | Asymmetric | ECC-256 | 256 bits | 1 year |
| System Authentication | Symmetric (HMAC) | HMAC-SHA256 | 256 bits | 1 year |

## 5. Compliance and Monitoring

- **Audit and Review:**
  - Cryptographic controls, key management, and related access must be periodically reviewed for continued effectiveness and compliance with applicable requirements.
  - Automated monitoring tools are used to log key usage and access events, and regular reviews ensure that cryptographic controls remain effective.

## 6. Exceptions

- **Documented Deviations:**
  - Any exceptions to this policy must be formally documented and submitted to the Information Security Officer or designated authority.
  - Exceptions are granted only after a thorough risk assessment and must include compensating controls to mitigate any potential risks.

## 7. Violations and Enforcement

- **Disciplinary Actions:**
  - Violations of this policy may result in disciplinary actions, including termination of employment or contractual agreements.
  - Unauthorized access to cryptographic keys or non-compliance with key management protocols will be investigated and addressed promptly, with corrective actions implemented to prevent future occurrences.