# Access Control Policy

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

APPROVED BY
Matt Sapio

## 1. Purpose

This policy defines requirements for managing and controlling access to Eigenomic's cloud-based systems, applications, AWS environment, and sensitive information. Its aim is to protect the confidentiality, integrity, and availability of information and support Eigenomic's SOC 2 security objectives.

## 2. Scope

This policy applies to all employees, contractors, vendors, and other authorized users who access Eigenomic systems, applications, AWS resources, or data. Eigenomic is a fully remote, cloud-based organization with fewer than five employees that develops custom automation software for law offices.

## 3. Access to Networks and Network Services

- **Cloud and Network Access Controls:**
  - Access to Eigenomic cloud resources, systems, applications, and network services is granted on a need-to-know and least privilege basis.
  - Appropriate AWS and application-level security controls must restrict access based on business need, role, and risk.
  - Sensitive data must be protected in transit and at rest using approved cryptographic controls, where applicable.

## 4. Customer Access Management

- **Limited Access:**
  - Customers receive access only to the services and data required to meet their contractual and regulatory needs.
  - Authentication and authorization mechanisms ensure that customers cannot access internal systems or sensitive data unrelated to their services.
  - Access is logged and periodically reviewed to detect any anomalies or unauthorized access attempts.

## 5. User Access Management

- **Access Provisioning:**
  - All access requests are subject to formal procedures that include verification, authorization by supervisors or designated authorities, and documentation.
  - Access rights are aligned with job responsibilities and are granted following a validated approval process.
  - Access to sensitive or customer data must be limited to authorized users with a legitimate business need.

## 6. User Registration and Deregistration

- **Formal Enrollment:**
  - Upon onboarding, users are registered with unique identifiers and their access rights defined according to their role.
  - Upon termination, role change, or contract completion, access must be promptly revoked or adjusted.
  - Records of registration and deregistration are maintained for audit purposes and compliance with applicable legal, contractual, and SOC 2 requirements.

## 7. User Access Provisioning and De-provisioning

- **Documented Procedures:**
  - Access provisioning is performed using documented procedures that include verification, approval, and logging of all activities.

- Regular audits ensure that access rights remain appropriate to the current job function, with any discrepancies corrected immediately.
- This process is coordinated with HR and department managers as part of employee lifecycle management.

## 8. Management of Privileged Access

- **Restricted Privileges:**
  - Access to privileged accounts is restricted to only those personnel whose roles require elevated access.
  - All privileged activities are continuously monitored and logged.
  - Users with privileged access must understand and comply with elevated-access security responsibilities.
  - Periodic reviews ensure that any unnecessary privileges are revoked and that all activities are in compliance with regulatory standards.

## 9. Periodic User Access Reviews

- **Regular Auditing:**
  - User accounts and access rights must be reviewed periodically and at a frequency appropriate to risk.
  - The review process includes validating access levels, ensuring alignment with current role responsibilities, and verifying compliance with applicable legal, contractual, and SOC 2 requirements.
  - Any deviations or excess privileges are immediately corrected.

## 10. Removal and Adjustment of Access Rights

- **Timely Modifications:**
  - Access rights are promptly adjusted or removed when user roles change or when users exit the organization.
  - This process is embedded within the offboarding procedure and coordinated with HR to maintain accurate access control records.

## 11. Segregation of Duties

- **Conflict of Interest Prevention:**
  - Where practical for an organization of Eigenomic's size, incompatible duties should be separated. Where full segregation is not practical, management must use documented oversight, review, or other compensating controls.
  - The policy ensures that key functions are separated to reduce the risk of misuse of privileges and to mitigate potential fraud, meeting both applicable legal, contractual, and SOC 2 requirements.

## 12. Management of Authentication Credentials

- **User Responsibilities:**
  - Users must protect the confidentiality of their authentication credentials, including passwords and security tokens.
  - Guidelines for secure storage and regular updates of credentials are enforced through technical measures.
  - Users are required to immediately report any suspected compromise of credentials.

## 13. Password Policy

- **Strong Password Guidelines:**
  - Passwords must meet Eigenomic's approved authentication standards and applicable system-enforced requirements.
  - Multi-factor authentication (MFA) must be used for privileged access and other systems where required by Eigenomic's security standards.
  - Authentication controls should be technically enforced where supported by the applicable system.

## 14. Information Access Restrictions

- **Controlled Access:**
  - Access to sensitive information is strictly limited to authorized personnel based on their role and need-to-know.

- Role-based access controls (RBAC) and encryption are implemented where appropriate.
- Attempts to access restricted information are logged and periodically reviewed to prevent unauthorized disclosures.

## 15. Secure Log-On Procedures

- **Secure Authentication:**
  - All log-on procedures enforce secure authentication methods, such as two-factor authentication (2FA) or equivalent measures.
  - Users are educated on the importance of following secure log-on practices and safeguarding their credentials.

## 16. Password Management System

- **Centralized Control:**
  - A dedicated password management system may be used to store and manage passwords securely.
  - The system enforces password policies, supports periodic password changes, and maintains a secure vault for sensitive credentials.
  - Access to this system is strictly limited to authorized personnel.

## 17. Use of Privileged Utility Programs

- **Controlled Use:**
  - Privileged utility programs that enable elevated system access are limited to essential usage only.
  - All usage of such programs is logged and subject to regular audits to ensure compliance with access control requirements.

## 18. Access to Program Source Code

- **Source Code Security:**
  - Access to program source code is restricted to authorized personnel only.

- Source code is stored in secure repositories with access controls and encryption.
- Any access must be justified, documented, and subject to periodic reviews to prevent unauthorized modifications.

## 19. Exceptions

- **Documented Exceptions:**
  - Any exceptions to this policy must be formally documented and approved by the Policy Owner or an authorized representative.
  - Exceptions are reviewed periodically to ensure they do not introduce undue compliance risks.

## 20. Violations and Enforcement

- **Consequences:**
  - Violations of this policy may result in disciplinary action, including termination of employment or contracts.
  - All violations will be investigated, with corrective actions implemented to prevent future occurrences.
  - Enforcement mechanisms ensure ongoing compliance with the guidelines and relevant regulatory requirements.