Elevaite365

Access Control Policy

Version 1.0

PURPOSE

This policy applies to all information systems, networks, applications, data, and physical facilities owned, managed, or operated by Elevaite365(hereby referred to as organization). It governs access for all employees, contractors, vendors, and third parties, ensuring security, operational integrity, and regulatory compliance.
This policy covers all environments—on-premises, cloud, remote access, and hybrid setups. It also covers access via organizational devices, personal devices, and any interfaces used to interact with organizational systems and data.

SCOPE

This policy defines the framework and establishes guidelines for controlling access to organizational resources. It ensures that access is granted and managed in a manner that prevents unauthorized access, protects sensitive data, and complies with regulatory requirements. By implementing robust access controls, the organization aims to minimize data breaches, unauthorized access, and potential system misuse risks.

DEFINITIONS

- **Access Control:** A security mechanism that regulates who or what can view or use resources in a computing environment. It involves processes for identification, authentication, and authorization.
- **Logical Access:** Refers to access granted via digital mechanisms, such as user accounts, passwords, and authentication tools.
- **Privileged Access:** Administrative or high-level access rights that provide elevated control over critical systems and data.
- **Least Privilege:** A security principle that ensures users are granted only the minimum level of access required to perform their job duties effectively.
- **Multi-Factor Authentication (MFA):** An authentication process that requires multiple verification forms to enhance security.
- **Single Sign-On (SSO):** An authentication mechanism allowing users to log in once to access multiple systems securely.
- **Information Security Group (ISG):** The team responsible for enforcing and overseeing information security measures, including access control.
- **Leadership Team (LT):** Senior management responsible for strategic decisions and compliance with security policies.

RESPONSIBILITIES

Implementing, monitoring, and maintaining this policy are the joint responsibilities of the Information Security Group (ISG) and other relevant teams, including IT administrators, system owners, and department heads. Specific responsibilities include:

1. **Information Security Group (ISG):**
    - Defining access control requirements and ensuring compliance.
    - Conducting periodic audits and access reviews.
    - Guiding privileged access management and access provisioning processes.
2. **IT Administrators and System Owners:**
    - Enforcing access control measures on all systems under their management.
    - Ensuring timely provisioning, modification, and revocation of access rights.
    - Maintaining detailed records of access activities for audit purposes.
3. **Department Heads and Managers:**
    - Approving access requests based on business requirements.

- Ensuring that employees adhere to the principle of least privilege.

4. **End Users:**

   - Protecting credentials and ensuring compliance with password and access guidelines.
   - Reporting any security incidents or unauthorized access promptly.

POLICY

Organizational Requirements for Access Management

The access management policy outlines the essential standards for granting, monitoring, and revoking access to systems, data, and resources. It ensures alignment with operational goals, security protocols, and regulatory requirements while minimizing risks. This structured approach supports secure and efficient access, balancing business needs with robust protection of critical assets.

1. **Least Privilege Principle**
   Access to systems, data, and resources is restricted to the minimum necessary for users to perform their job functions. Any permissions beyond operational requirements must be eliminated to reduce security risks and maintain system integrity.

2. **Role-Based Access Control (RBAC)**
   Access rights are assigned based on predefined roles within the organization. This ensures that permissions align with job responsibilities and access control processes remain efficient and scalable.

3. **Accountability and Traceability**
   To ensure accountability, all access actions must be uniquely attributable to individual users. Shared accounts are prohibited unless explicitly approved, justified, and documented for specific use cases.

4. **Separation of Duties**
   Responsibilities must be distributed to prevent unauthorized or unintended actions. Critical processes must not be controlled end-to-end by a single individual; for instance, the individual initiating a transaction cannot also approve it.

5. **Secure Authentication**
   Access to critical systems requires robust authentication measures. To enhance security and verify user identities, sensitive systems must implement multi-factor authentication (MFA).

6. **Auditable Actions**
   All-access activities must be logged and retained to support compliance, auditing, and incident investigations. Logs must include sufficient detail to allow traceability and identify unauthorized or suspicious actions.

User Access Management

A structured approach to managing user access is critical for maintaining security and operational control. The following procedures must be implemented:

Access Request and Approval

1. Access requests must be submitted via the Microsoft Devops or through an approved email.
2. Requests must include:
   a. The requester’s full name, department, and role.
   b. A clear and detailed justification for access, specifying the systems, data, or resources required.
   c. Approval from the requester’s manager or department head is required to verify the request’s alignment with job responsibilities.

Account Creation and Configuration

1. Unique user accounts must be created for each individual, ensuring traceability and accountability.
2. Default vendor accounts and system-generated accounts must be disabled or removed before system deployment.
3. User accounts must enforce:

   a. Strong password policies.

   b. Automatic session timeouts after periods of inactivity.

   c. Lockouts after multiple failed login attempts.

Inactive and Dormant Accounts

1. Accounts not accessed for the 180 Days must be flagged for review and deactivated unless explicitly justified.

2. New, unused accounts for 120 Days post-creation must be disabled unless formally reactivated.

Periodic Access Reviews

1. Quarterly system owners and managers must conduct periodic reviews of all user access rights to ensure permissions align with current job responsibilities.

2. Access must be immediately adjusted for employees who undergo role changes, such as promotions, demotions, or lateral transfers.

Account Termination

1. Access for terminated employees, contractors, or third parties must be revoked within the 30 Days of HR or management notification.

2. IT administrators must document all account deactivations for audit purposes.

Privileged Access Management

Privileged accounts grant elevated permissions and must be managed with enhanced controls to mitigate risks.

Privileged Account Standards

1. Privileged accounts must only be granted to users with a documented business need for elevated permissions.

2. Administrative tasks must be performed using dedicated privileged accounts separate from standard user accounts.

Authentication and Security Controls

1. MFA is mandatory for all privileged accounts to add a layer of security.

2. Privileged account passwords must:

   a. Be at least 10 Characters long.

   b. Include a mix of uppercase, lowercase, numbers, and special characters.

   c. Be rotated every 180 Days.

Temporary Privileged Access

1. Temporary access to privileged accounts must have predefined expiration dates and be revoked automatically upon task completion.

2. All activities performed during temporary privileged access must be logged and reviewed.

Activity Logging and Auditing

1. All privileged account activities, such as configuration changes and data access, must be logged.

2. Logs must be reviewed monthly by IT or security personnel to detect unauthorized or suspicious activities.

Access to Networks and Network Services
Network Access Controls

1. Network access requests must be formally documented, including:
    a. The user's role, the purpose of access, and the system to be accessed.
    b. The approver and access validity period.
2. Access to production networks is limited to authorized personnel with valid business needs.

Guest Access

1. Guests may access isolated networks explicitly designed for visitor use. Registration in the visitor register is mandatory, and guest networks must remain segregated from production environments.

Remote Access

1. All remote access must use encrypted communication protocols like VPN, TLS, or IPsec.
2. MFA is required for all remote connections.
3. Remote access logs must be retained for a minimum of 90 Days and reviewed periodically for anomalies.

Password and Authentication Standards
Passwords are a critical component of authentication and must meet the following requirements:

1. Passwords must:
    - Be at least 10 Characters long.
    - Include uppercase and lowercase letters, numbers, and special characters.
    - Avoid dictionary words, usernames, or easily guessable sequences.
2. Accounts must:
    - Lock after 10 failed login attempts.
    - Enforce password rotation every 180 Days.
3. Passwords must be stored securely using cryptographic hashing algorithms. Plaintext storage or transmission is strictly prohibited.

Monitoring and Auditing

1. **Activity Logging**
    a. All-access events, including logins, privilege escalations, and configuration changes, must be logged with sufficient detail, including timestamps, user IDs, and activity descriptions.
    b. Logs must be securely stored for 90 Days to support audits and investigations
2. **Periodic Audits**
    a. Quarterly user and privileged access audits must ensure compliance with access control policies.
    b. The IT security team must review privileged activity logs monthly to identify anomalies.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-