Access Control Policy Template

Document Control Information

- **Document Title:** Access Control Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Access Control Policy establishes [ORGANIZATION NAME]'s approach to managing access to information systems and data in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that access to information assets is appropriately authorized, controlled, and monitored.

1.2 Scope

This policy applies to all access to information systems, applications, data, and facilities within [ORGANIZATION NAME], including: - All information systems and applications - All data repositories and storage systems - All network infrastructure and communication systems - All physical facilities housing information assets - All employees, contractors, consultants, temporary staff, and other workers - All third parties requiring access to [ORGANIZATION NAME]'s information systems

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing access controls based on business and security requirements - Ensuring access rights follow the principle of least privilege - Regularly reviewing and updating access rights - Maintaining segregation of duties where appropriate - Protecting systems and information from unauthorized access

2. Access Control Principles

2.1 Need-to-Know

Access to information shall be granted only to individuals who require it to perform their job functions or fulfill their contractual obligations.

2.2 Least Privilege

Users shall be provided with the minimum access rights necessary to perform their job functions or fulfill their contractual obligations.

2.3 Segregation of Duties

Conflicting duties and areas of responsibility shall be separated to reduce opportunities for unauthorized or unintentional modification or misuse of information assets.

2.4 Default Deny

Access to systems and information shall be denied by default unless explicitly granted.

3. User Access Management

3.1 User Registration and Deregistration

[ORGANIZATION NAME] shall implement a formal user registration and deregistration process that includes: - Verification of user identity - Verification of access requirements - Assignment of unique user identifiers - Obtaining management approval for access requests - Maintenance of a record of authorized users - Prompt removal or disabling of access rights upon termination or change of employment

3.2 User Access Provisioning

The allocation and use of access rights shall be restricted and controlled through a formal access provisioning process that includes: - Using formal access request procedures - Requiring management authorization for access requests - Maintaining records of access rights granted - Configuring access rights according to the principle of least privilege - Regularly reviewing and updating access rights

3.3 Management of Privileged Access Rights

The allocation and use of privileged access rights shall be restricted and controlled through: - Formal authorization for privileged access rights - Verification of competence for privileged users - Maintenance of a record of privileged users - Regular review of privileged access rights - Implementation of enhanced controls for privileged accounts - Use of dedicated administrator accounts for administrative activities

3.4 Review of User Access Rights

[ORGANIZATION NAME] shall review users' access rights at regular intervals and after any changes, such as: - Promotion, demotion, or transfer to another department - Termination of employment or contract - Changes to system or application access requirements - Organizational changes

4. User Responsibilities

4.1 Password Management

Users shall follow good security practices in the selection and use of passwords, including: - Keeping passwords confidential - Avoiding the use of the same password for different systems - Changing passwords when there is any indication of possible compromise - Selecting strong passwords according to the Password Policy - Changing temporary passwords at first log-on

4.2 Unattended User Equipment

Users shall ensure that unattended equipment has appropriate protection, including: - Logging off or locking systems when unattended - Protecting devices with screen locks and password protection - Securing physical documents and removable media - Implementing automatic screen locking after a defined period of inactivity

5. Network Access Control

5.1 Network Segmentation

[ORGANIZATION NAME] shall segregate networks based on security requirements, including: - Separation of internal and external networks - Segregation of sensitive systems and data - Implementation of network access controls between segments - Regular review and validation of network segmentation

5.2 Network Connection Control

Access to internal and external networked services shall be controlled through: - Network access policies and procedures - Authentication mechanisms for connections to networks - Monitoring and control of remote access - Restriction of connection capabilities for users and equipment

5.3 Wireless Network Security

Wireless networks shall be secured through: - Strong encryption protocols - Secure authentication methods - Segregation from internal networks where appropriate - Regular security assessments of wireless networks

6. Operating System and Application Access Control

6.1 Secure Log-on Procedures

Access to operating systems and applications shall be controlled by secure log-on procedures, including: - Displaying a general notice warning that the system is for authorized users only - Not displaying system or application identifiers until the log-on process is successfully completed - Validating log-on information only on completion of all input data - Protecting against brute force log-on attempts - Logging unsuccessful log-on attempts - Not transmitting passwords in clear text

6.2 User Authentication

[ORGANIZATION NAME] shall implement appropriate authentication mechanisms based on risk assessment, including: - Password-based authentication with strong password requirements - Multi-factor authentication for sensitive systems and remote access - Biometric authentication where appropriate - Certificate-based authentication where appropriate

6.3 Session Management

[ORGANIZATION NAME] shall implement controls to manage user sessions, including: - Session timeout after a defined period of inactivity - Restrictions on concurrent sessions - Secure session establishment and management - Session termination after completion of activity

7. Information Access Restriction

7.1 Information Classification and Handling

Access to information shall be restricted in accordance with the Information Classification Policy, including: - Defining access restrictions based on classification levels - Implementing appropriate controls for each classification level - Regularly reviewing and updating classification levels - Training users on information handling requirements

7.2 Application and Information Access Control

[ORGANIZATION NAME] shall restrict access to application functions and data according to: - Defined access control policies - Business requirements for access - Regulatory and contractual requirements - Risk assessment results

8. Remote Access and Mobile Computing

8.1 Remote Access

Remote access to [ORGANIZATION NAME]'s networks and systems shall be controlled through: - Formal authorization procedures - Strong authentication mechanisms - Encrypted communication channels - Restriction of activities that can be performed remotely - Logging and monitoring of remote access activities

8.2 Mobile Computing

Security shall be applied when using mobile computing facilities, including: - Protection of mobile devices with encryption and access controls - Secure connectivity for mobile devices - Restrictions on applications and data stored on mobile devices - Remote wipe capabilities for lost or stolen devices

9. Third-Party Access

9.1 Third-Party Access Requirements

Access by third parties to [ORGANIZATION NAME]'s information systems shall be controlled through: - Risk assessment prior to granting access - Formal contracts and agreements with security requirements - Limited access based on business requirements - Monitoring and review of third-party activities - Termination of access upon completion of the agreement

9.2 Outsourced Development and Support

Access by outsourced development and support personnel shall be controlled through: - Supervised access for development and support activities - Review of code and changes before implementation - Segregation of development, test, and production environments - Restriction of access to production data

10. Access Control Monitoring and Audit

10.1 Logging and Monitoring

[ORGANIZATION NAME] shall implement logging and monitoring of access control activities, including: - User activities, exceptions, and security events - System administrator and operator activities - Successful and rejected system access attempts - Changes to access rights and privileges - Use of privileged utility programs

10.2 Clock Synchronization

System clocks shall be synchronized to ensure accurate time stamps for access control logs and audit trails.

10.3 Access Control Audit

Regular audits of access control measures shall be conducted to verify: - Compliance with this policy - Effectiveness of access control mechanisms - Appropriate allocation of access rights - Timely removal of access rights when no longer required

11. Compliance and Exceptions

11.1 Compliance Measurement

Compliance with this policy shall be verified through: - Regular access reviews - Internal and external audits - Automated compliance monitoring tools - Security assessments and penetration testing

11.2 Exceptions

Exceptions to this policy shall be: - Documented and recorded - Approved by appropriate management - Time-limited and regularly reviewed - Risk-assessed and with compensating controls where necessary

12. Related Documents

- Information Security Policy
- Password Policy
- Information Classification Policy
- Remote Working Policy
- Third-Party Security Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

13. Approval

This Access Control Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____