iGUIDE

ISMS

Information Security Access Control

iNFOSECBASE

Contents

A Guide to Information Security Access Control

Introduction

Access control is a fundamental component of ISO 27001, ensuring that only authorised individuals can access systems, networks and data. Poor access control can lead to unauthorised access, data breaches and security threats. Organisations must implement identity management, authentication mechanisms and access rights to safeguard information assets.

This guide outlines ISO 27001 requirements for access control, including identity management, authentication information and access rights, along with best practices for implementation.

Purpose of Access Control

Effective access control ensures that:

- Only authorised users can access sensitive systems and data.
- Authentication and verification mechanisms are in place to prevent unauthorised access.
- Access rights are managed and regularly reviewed to align with business needs.
- Compliance with security policies and regulations (e.g. GDPR, NIST, HIPAA) is maintained.

Key ISO 27001 Requirements for Access Control

Organisations must:

- Establish an Access Control Policy defining rules for user access.
- Implement identity and authentication management to verify users.
- Assign access rights based on job roles and the principle of least privilege.
- Use multi-factor authentication (MFA) for enhanced security.
- Monitor and review user access logs to detect unauthorised activities.
- Regularly audit and update access control measures.

Key Security Requirements for Privileged Access Rights

Organisations must:

- Limit privileged access to only those who require it for their job roles.
- Implement role-based access control (RBAC) to ensure privileges align with business needs.
- Enforce multi-factor authentication (MFA) for privileged accounts.
- Maintain an inventory of privileged users and regularly review their access rights.
- Monitor and log privileged activities to detect and prevent misuse.
- Use separate accounts for administrative tasks and standard user activities.
- Regularly review and revoke unnecessary privileges to reduce risk exposure.

Key Requirements for Information Access Restriction

Organisations must:

- Define access control policies based on the principle of least privilege (PoLP) and need-to-know basis.
- Implement role-based access control (RBAC) to limit access based on job responsibilities.
- Use technical measures such as authentication, encryption and logging to monitor and control access.
- Regularly review and update access permissions to ensure only authorised individuals have access.
- Apply multi-factor authentication (MFA) where necessary for enhanced security.

Key Requirements for Access to Source Code

Organisations must:

- Restrict access to source code based on business needs and security principles (e.g. least privilege and need-to-know).
- Use version control systems (VCS) (e.g. Git, SVN) with access controls and logging.
- Monitor and log all access and modifications to source code repositories.
- Implement secure authentication methods, such as multi-factor authentication (MFA), for accessing source code.
- Prevent unauthorised code changes through change management and peer review processes.

Key Requirements for Secure Authentication

Organisations must:

- Enforce strong authentication mechanisms, such as multi-factor authentication (MFA) for critical systems.
- Implement secure password policies, including complexity requirements, expiration periods and password reuse restrictions.
- Use secure authentication methods, such as biometrics, smart cards or hardware security tokens when appropriate.
- Protect authentication credentials by storing passwords securely using hashing and salting techniques.
- Monitor authentication attempts and detect suspicious login activities, such as multiple failed attempts.

Implementing Access Control

Identity Management

Identity management ensures that users have unique, verifiable identities before granting access. Key measures include:

- **User Enrolment**: Establish a process for registering new users and verifying their identity.
- **Role-Based Access Control (RBAC)**: Assign access based on job roles to prevent excessive permissions.
- **User Lifecycle Management**: Implement procedures for onboarding, modifying and revoking access.
- **Privileged Access Management (PAM)**: Secure administrative accounts with stricter controls.

Authentication Information

Authentication mechanisms verify that users are who they claim to be. Best practices include:

- **Multi-Factor Authentication (MFA)**: Require two or more verification factors (e.g. password plus mobile/email one-time-password [OTP]).
- **Strong Password Policies**: Enforce complex passwords with expiration and rotation policies.
- **Biometric Authentication**: Use fingerprint, facial recognition or other biometric factors.
- **Single Sign-On (SSO)**: Enable secure, centralised authentication across multiple systems.

Access Rights Management

Controlling access rights minimises the risk of unauthorised access and data exposure. Organisations should:

- **Apply the Principle of Least Privilege (PoLP)**: Grant users only the minimum access needed for their role.
- **Regularly Review Access Rights**: Conduct periodic access reviews to remove unnecessary privileges.
- **Monitor User Activity**: Log and analyse user actions to detect anomalies or unauthorised access.
- **Enforce Segregation of Duties (SoD)**: Prevent conflicts of interest by ensuring critical tasks require multiple approvals.

Monitoring and Auditing Access Control

- **Log all access events** (successful and failed login attempts, privilege escalations).
- **Use security monitoring tools** (SIEM) to detect suspicious activity.
- **Conduct periodic audits** to validate access compliance with policies.
- **Perform regular penetration testing** to identify access control vulnerabilities.

Best Practices for Secure Access Control

- Implement **Zero Trust security principles** (never trust, always verify).
- Enforce **automatic session timeouts** for inactive users.
- Secure **remote access** using VPNs, firewalls and endpoint protection.
- Use **just-in-time (JIT) access** to grant temporary, time-limited permissions.

- Train employees on **security awareness** and **phishing prevention**.

Summary

Access control is a critical aspect of ISO 27001, ensuring that only authorised individuals can access information systems and sensitive data. Organisations must implement identity management, authentication mechanisms and access rights to protect against unauthorised access and security breaches.

Identity management involves user registration, role-based access control (RBAC) and privileged access management (PAM). Authentication information includes multi-factor authentication (MFA), strong password policies and biometric verification. Access rights management enforces the principle of least privilege (PoLP), regular access reviews and segregation of duties (SoD) to minimise security risks.

Regular monitoring, logging and auditing of access control measures help detect anomalies and unauthorised activity. Implementing Zero Trust principles, remote access security and user awareness training further strengthens access control. By adopting these best practices, organisations can enhance security, ensure compliance and safeguard critical information assets.