Access Control Standards

Access Control Principles

Least privilege: Users have minimum access needed for their role. Need-to-know: Access granted only for legitimate business need.

Separation of duties: No single user has excessive privileges. Regular access reviews ensure appropriate access.

User Account Management

Unique user accounts for each person. No shared accounts except approved service accounts.

Account creation requires manager approval. Access provisioned based on role and department. Accounts disabled immediately upon termination.

Authentication Requirements

Strong passwords required (12+ characters, complexity). Multi-factor authentication (MFA) mandatory for all systems.

Biometric authentication encouraged where available. Single sign-on (SSO) for integrated systems.

Authorization Levels

Read-only: View data but cannot modify. User: Standard access for role. Power user: Additional capabilities for advanced users.

Administrator: Full system control. Granted sparingly with approval. Privileged access monitored closely.

Role-Based Access Control

Access assigned based on job role. Standard roles defined for common positions.

Custom roles for unique requirements. Role changes trigger access review and adjustment.

Access Request Process

Submit access requests through IT portal. Include: System, access level, business justification.

Manager approval required. Additional approval for privileged access. Access provisioned within 1 business day.

Access Reviews

Quarterly access reviews by managers. Verify each user's access is still appropriate.

Remove unnecessary access. Document review completion. Audit tracks review compliance.

Privileged Access Management

Privileged accounts (admin, root) require additional controls. Just-in-time access: Elevated privileges granted temporarily when needed.

Privileged sessions recorded. Regular audits of privileged account usage.

Service Accounts

Service accounts for automated processes and applications. Strong passwords (20+ characters). Stored in password manager.

Access restricted to authorized personnel. Regular password rotation. Document service account purpose and owner.

Remote Access Control

VPN required for remote access to company resources. MFA enforced for VPN connections.

Remote desktop access restricted to approved users. Session timeouts for inactive connections.

Physical Access Control

Badge access to office facilities. Visitor sign-in and escort required.

Server room access restricted to authorized IT personnel. Access logs reviewed monthly.

Access Termination

Immediate access revocation upon termination. Disable accounts, revoke VPN, collect badges and devices.

Transfer data ownership before departure. Document access removal completion.

Guest and Contractor Access

Temporary accounts for contractors and guests. Limited access based on need.

Sponsor responsible for guest access. Access expires automatically. Regular review of active guest accounts.

Access Monitoring

Log all access to sensitive systems and data. Monitor for unusual access patterns.

Alert on: After-hours access, failed login attempts, privilege escalation, access from unusual locations.

Access Violations

Report access violations to security team. Investigate unauthorized access attempts.

Violations may result in disciplinary action. Repeated violations may lead to termination.

Compliance Requirements

Access controls comply with regulatory requirements (SOX, GDPR, HIPAA where applicable).

Document access control procedures. Demonstrate compliance during audits.