Information Security Policy

Security Principles

Protect company and customer data through confidentiality, integrity, and availability. Security is everyone's responsibility.

Follow the principle of least privilege - access only what you need for your role. Report security concerns immediately.

Access Control

User accounts are personal and non-transferable. Never share passwords or login credentials. Use strong, unique passwords for each system.

Multi-factor authentication (MFA) is required for all systems. Access is granted based on role and revoked upon termination or role change.

Password Requirements

Passwords must be at least 12 characters with uppercase, lowercase, numbers, and special characters. Don't reuse passwords across systems.

Change passwords immediately if compromised. Use the company password manager to generate and store passwords securely.

Data Classification

Data is classified as Public, Internal, Confidential, or Restricted. Handle data according to its classification level.

Confidential and Restricted data requires encryption in transit and at rest. Don't store sensitive data on personal devices or unauthorized cloud services.

Physical Security

Lock your computer when leaving your desk. Don't leave devices unattended in public places. Secure printed confidential documents.

Visitors must be escorted in office areas. Report tailgating or unauthorized persons to security immediately.

Incident Reporting

Report security incidents including suspected malware, phishing, data breaches, or policy violations to security@company.com immediately.

Don't attempt to investigate or remediate incidents yourself. Preserve evidence and follow security team instructions.

Remote Access

Use company VPN for all remote access to company resources. Don't access company systems from public or unsecured networks without VPN.

Ensure your home network is secured. Don't allow others to use company devices or access company systems through your credentials.

Third-Party Security

Vendors and partners with access to company systems or data must comply with our security requirements and sign appropriate agreements.

Don't share company data with third parties without proper authorization and data protection agreements.

Security Training

All employees must complete annual security awareness training. Additional role-specific training may be required.

Stay informed about current threats and security best practices. When in doubt, ask the security team.

Compliance and Audits

Comply with all security audits and assessments. Provide requested information and access to auditors promptly.

Security policies are reviewed annually and updated as needed. You'll be notified of significant changes.