Information Security & Acceptable Use Policy

ABC Company - Internal Policy Document

Field	Value
Document ID	ABC-POL-275
Version	1.0
Effective Date	01 Jan 2026
Owner	Security & IT
Review Cycle	Annual
Approved By	HR & Compliance

This document outlines company policies and procedures for ABC employees and contractors. It is intended for internal reference. If you have questions, contact the document owner.

1. Purpose & Scope

This policy establishes minimum information security requirements for ABC Company systems, data, and devices.

- Applies to: employees, contractors, and vendors with access to ABC data
- Covers: corporate accounts, endpoints, networks, and SaaS tools
- Security incidents must be reported immediately (see Section 6)

2. Account Security

- Multi-factor authentication (MFA) is required for email, source control, and finance tools
- Passwords must be at least 12 characters and include a mix of character types
- Do not reuse passwords across personal and corporate accounts
- Use the approved password manager to store credentials

3. Data Classification & Handling

All information must be classified and handled accordingly.

Data Classification	Examples	Handling Requirements
Public	Marketing content, press releases	May be shared externally after review.
Internal	Org charts, internal announcements	Share only within ABC; avoid public links.
Confidential	Customer data, contracts, financials	Encrypt in transit and at rest; need-to-know access.
Restricted	Credentials, security keys, regulated data	Strong encryption; access logged; strict approval required.

4. Device & Remote Work Security

- Company laptops must have full-disk encryption enabled
- Install security updates within 7 days of release (or sooner for critical patches)
- Use VPN on untrusted networks (public Wi-Fi)

- Do not store Confidential/Restricted data on personal devices unless explicitly approved

5. Email & Phishing

- Verify payment/bank change requests via a second channel
- Report suspicious emails using the 'Report Phishing' button or forward to security@abc.example
- Do not click unknown links or open unexpected attachments

6. Incident Reporting

If you suspect a breach, lost device, or unauthorized access, report immediately.

- Step 1: Disconnect affected device from network (if safe to do so)
- Step 2: Notify security@abc.example and your manager within 30 minutes
- Step 3: Preserve evidence (do not delete files/logs)
- Step 4: Follow Security team's instructions for remediation

7. Enforcement

Violations may result in access revocation and disciplinary action up to termination and legal action.