

Acceptable Use Policy

Purpose

Your Organization provides information systems, networks, devices, and communication tools to support its business. This policy defines acceptable and prohibited use of those resources so that workforce members understand their responsibilities, Your Organization can meet its legal and contractual obligations, and the organization's information assets stay protected against misuse, disclosure, or damage.

Scope

This policy applies to all workforce members of Your Organization, including full-time and part-time employees, contractors, consultants, temporary workers, and interns ("users"). It covers all Your Organization-owned or -managed information systems, corporate email, productivity and collaboration tools, laptops and mobile devices, cloud services provisioned by Your Organization, the corporate network, and any personal device used to access corporate resources under a bring-your-own-device arrangement.

General principles

- **Business use.** Your Organization resources are provided primarily for business use. Limited, occasional personal use is permitted provided it does not interfere with work, consume excessive resources, or violate any term of this policy.
- **No expectation of privacy.** Subject to applicable law, users should have no expectation of privacy when using Your Organization systems. Your Organization may monitor, inspect, and log activity for security, compliance, and troubleshooting purposes.
- **Accountability.** Users are responsible for all activity originating from their accounts and are accountable for safeguarding their credentials.

Acceptable use

Users must:

- Use strong, unique passwords and enable multi-factor authentication on every account that supports it.
- Lock unattended workstations and devices.
- Report suspected security incidents, lost or stolen devices, and phishing attempts to the security team promptly.
- Encrypt sensitive data in transit and at rest using Your Organization-approved tools.
- Connect to the corporate network only from devices that meet Your Organization endpoint standards (patched, anti-malware enabled, disk encryption on).
- Complete assigned security-awareness training and annual acceptable-use policy acknowledgment.

Prohibited activities

Users must not:

- Share account credentials with any person for any reason.
- Install or use unlicensed, cracked, or unauthorized software on corporate devices.
- Disable, circumvent, or tamper with security controls (antivirus, firewall, DLP, MDM, monitoring agents).
- Use Your Organization systems to store, process, or transmit personal cryptocurrency wallets, personal side-business data, or unlawful content.
- Access, download, transmit, or store harassing, discriminatory, obscene, or otherwise objectionable material.
- Attempt to gain unauthorized access to systems, accounts, or data — internal or external — outside the scope of an authorized job duty.
- Conduct personal commercial activity, political campaigning, or fundraising using corporate resources.

Remote work and mobile devices

Users working remotely must use Your Organization-approved VPN or zero-trust access tools to reach internal resources. Mobile devices that access corporate data must be enrolled in the Your Organization MDM solution and must maintain a screen lock with auto-lock no longer than five minutes. Lost or stolen devices must be reported within 24 hours so the device can be remotely wiped.

Email, messaging, and social media

Corporate email and chat are subject to retention and legal-hold obligations. Users must not auto-forward corporate email to personal accounts. When representing Your Organization on social media, users must comply with the Communications and Brand policies.

Enforcement

Violations of this policy may result in disciplinary action up to and including termination, and may be referred to law enforcement where applicable. Access may be suspended during investigation of a suspected violation.

Scope exceptions

Exceptions to this policy must be requested in writing to the Information Security team, must describe the compensating controls, and must be approved by the CISO or designee.

Review cadence

This policy is reviewed annually by the Information Security team and the policy owner, or sooner if a material change occurs in Your Organization's business, technology, or regulatory environment.

Effective date: [the date this policy takes effect]