



Acceptable Use Policy (AUP)

The Acceptable Use Policy (AUP) defines the proper use of company technology, internet, email, and social media. This policy establishes guidelines to ensure that all employees, contractors, and authorized users understand their responsibilities when accessing and using company-provided systems and resources.

Purpose

The purpose of this policy is to protect the organization's digital assets, reduce the risk of insider threats, prevent shadow IT practices, and avoid misuse of company resources that could result in security vulnerabilities, data breaches, or reputational damage.

Scope

This policy applies to all employees, contractors, vendors, and third parties who access the organization's technology systems, including but not limited to computers, mobile devices, email accounts, internet services, and social media platforms used for business purposes.

Policy Guidelines

- Company resources are to be used primarily for business-related activities.
- Personal use of company technology must be limited and not interfere with work responsibilities.
- Users must not install unauthorized software or connect unapproved devices to the network.
- Accessing or sharing inappropriate, offensive, or illegal content is strictly prohibited.
- Company email and communication channels must not be used for harassment, spamming, or phishing.
- Employees are expected to protect login credentials and not share them with unauthorized individuals.
- Use of cloud storage and external drives must comply with company security standards.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, as well as legal action where applicable.

Acknowledgment

All employees and users must acknowledge that they have read, understood, and agreed to comply with this Acceptable Use Policy before being granted access to company systems and resources.