ACCEPTABLE USE POLICY (AUP)

Version 1.0 — For Software/IT Teams

1. Purpose

This policy defines acceptable and unacceptable use of company-owned devices, networks, and software systems.

2. Scope

Applies to all employees, interns, contractors, and third parties using company IT assets.

3. General Acceptable Use

- Use company systems primarily for business purposes.

- Limited personal use is allowed if it does not affect productivity or security.

- Report suspicious emails, phishing attempts, or security issues immediately.

4. Prohibited Activities

Users must NOT:

- Install unapproved software or browser extensions.

- Upload company code, designs, or data to personal cloud accounts.

- Store production data on personal devices.

- Bypass security controls (MFA, antivirus, VPN).

- Use company devices to access illegal or inappropriate content.

- Use AI tools to upload confidential code/data without approval.

5. Software Usage Rules

- Only IT-approved software may be installed.

- Developers may not use cracked or pirated software.

- GitHub access must follow code repository access rules.

6. Data Protection

- No sharing of confidential files via WhatsApp, Gmail, or personal drives.

- Only approved data transfer tools.
- Highly Confidential data must be encrypted.

7. Monitoring

The company may monitor system usage for security and compliance.

8. Violations

Breaches may lead to disciplinary action.

DATA CLASSIFICATION POLICY

Version 1.0

1. Purpose

Defines how company information is classified and handled.

2. Classification Levels

Public, Internal, Confidential, Highly Confidential.

3. Handling Requirements

Public: no restrictions.

Internal: internal sharing only.

Confidential: needs encryption.

Highly Confidential: strict need■to■know + encryption.

4. Disposal

Shred physical docs, securely delete digital files.

PASSWORD & ACCESS MANAGEMENT POLICY

Version 1.0

Password requirements: 12+ chars, complexity, no reuse, no sharing.

MFA: mandatory for email, VPN, production.

Privileged access: granted by IT only.

Offboarding: revoke access within 4 hours.

CHANGE MANAGEMENT POLICY

Version 1.0

Types of changes: Standard, Normal, Emergency.

Production change requirements: PR review, CI/CD checks, lead approval.

Rollback plan required.

SECURE CODING GUIDELINES

Version 1.0

- Follow OWASP Top 10.
- No hard-coded credentials.
- Validate all inputs.
- RBAC for authorization.
- Use secrets managers.
- No sensitive data in logs.
- Dependency scanning required.
- PRs require security review.

DEPLOYMENT & INFRASTRUCTURE ACCESS POLICY

Version 1.0

Deployment rules: authorized engineers only, CI/CD required.

Server access: VPN + unique SSH keys.

Backups: daily + weekly restore tests.