ACCEPTABLE USE POLICY (AUP)

Version: 1.0
Last Updated: January 2024
Owner: Operations Manager
Approved By: CEO

1. Purpose

The Acceptable Use Policy establishes the responsibilities and acceptable behaviors expected of all employees, contractors, and users accessing company systems, networks, and data. The primary purpose is to ensure technology resources are used safely, legally, and responsibly.

2. Scope

This policy applies to:

- Company-owned laptops, desktops, and mobile devices
- Cloud applications (Microsoft 365, CRM, Accounting SaaS)
- Company email and communication platforms
- Internet access provided through company networks

This policy does NOT explicitly cover:

- Personal devices used for work
- Employee-owned phones used for email

3. General Acceptable Use Requirements

Employees must:

- Use company systems primarily for business purposes
- Maintain the confidentiality of sensitive information
- Follow password and access control requirements
- Report suspicious activity or potential threats

4. Unacceptable Use

Users may not:

- Access or share inappropriate, offensive, or illegal content
- Install unauthorized software
- Attempt to bypass security controls
- Disable antivirus or monitoring tools
- Use company assets to conduct personal business ventures

5. Email & Communication Rules

Employees must:

- Avoid sharing sensitive data via personal email accounts
- Not use email to send large customer data files
- Avoid clicking suspicious links
- Use professional language in business communications

6. Use of Company Devices

Company devices must:

- Be kept updated with provided patches
- Be physically protected from theft or loss
- Never be shared with family members

7. Personal Devices (BYOD)

Employees may use their personal phones to:

- Check company email
- Access Microsoft Teams
- Access some SaaS applications

8. Software Use

Permitted:

- Approved business applications
- Cloud SaaS tools approved by department leads

Not permitted:

- Downloading unlicensed software

- Torrenting or file sharing
- Using personal accounts for storing company files

9. Internet Usage

Acceptable use includes:

- Accessing business tools
- Research related to work tasks

Unacceptable use includes:

- Streaming services unrelated to work
- High-bandwidth gaming
- Cryptocurrency mining
- Adult or illegal content

10. Data Security Responsibilities

Employees must:

- Store files only in approved cloud systems
- Protect sensitive information (PII, financial data)
- Not download customer data to personal devices

11. Physical Security Responsibilities

Employees must:

- Keep laptops secured when leaving the workplace
- Lock screens when away from desks
- Report lost or stolen devices immediately

12. Monitoring & Privacy Expectations

The company may monitor:

- Network activity
- Email communications
- System logs

13. Enforcement

Violations may result in:

- Verbal or written warnings
- Access restrictions
- Termination for serious violations

14. Policy Review

This policy should be reviewed annually or when major technology changes occur.

15. Approval

Approved by: CEO
Approval Date: January 2024