[Company Name] Acceptable Use Policy

**Document Version:** 1.0 **Date:** March 7, 2025

## 1. Overview

This Acceptable Use Policy (AUP) outlines the acceptable use of [Company Name]’s information technology (IT) resources. It applies to all employees, contractors, vendors, and any other individuals granted access to company systems, networks, data, or devices. The goal is to protect the company, its employees, its clients, and its assets from harm arising from inappropriate use of technology.

## 2. Purpose

The purpose of this policy is to:

* Define acceptable and unacceptable uses of company IT resources.
* Protect the confidentiality, integrity, and availability of company data and systems.
* Ensure compliance with all applicable laws and regulations.
* Minimize legal and security risks associated with technology use.
* Promote a productive and respectful work environment.

## 3. Scope

This policy applies to all company-owned or leased IT resources, and to any personally-owned devices used to access company data or networks (see also the Remote Work & BYOD Policy). This includes, but is not limited to:

* **Devices:** Computers (desktops, laptops), servers, mobile devices (phones, tablets), network equipment (routers, firewalls).
* **Networks:** Company wired and wireless networks, internet access.
* **Software:** Operating systems, applications, cloud-based services.
* **Data:** Electronic data (files, emails, databases), company information, client information.
* **Communication Tools:** Email, instant messaging, video conferencing.

## 4. Policy

### 4.1. General Principles

* Use of [Company Name]’s IT resources is a privilege, not a right.
* All users are expected to act responsibly, ethically, and legally.
* Users must prioritize the security and integrity of company systems and data.
* Users must respect the privacy of others.
* Company IT resources are primarily for business use. Limited personal use is permitted, but it must not violate this policy or interfere with work responsibilities. (See section 4.3)

### 4.2. Acceptable Use

The following activities are generally permitted, provided they comply with the General Principles (4.1) and all other sections of this policy:

* Work-related communication and collaboration.
* Accessing information necessary to perform job duties.
* Using company-approved software and applications.
* Storing and sharing work-related data securely.
* Accessing professional development resources.

### 4.3. Unacceptable Use

The following activities are strictly prohibited:

* **4.3.1. Illegal Activities:**
  + Using company resources for any illegal purpose.
  + Downloading, distributing, or accessing illegal content (e.g., child pornography, pirated software).
  + Engaging in any form of online fraud or harassment.
* **4.3.2. Security Violations:**
  + Attempting to bypass security controls.
  + Sharing passwords or access credentials.
  + Installing unauthorized software or hardware.
  + Disabling security features (e.g., antivirus).
  + Connecting unauthorized devices to the company network.
  + Intentionally introducing malware.
* **4.3.3. Harassment and Discrimination:**
  + Sending or displaying offensive, harassing, or discriminatory content.
  + Creating a hostile work environment.
* **4.3.4. Misrepresentation and Impersonation:**
  + Falsely representing oneself or the company.
  + Impersonating another user.
* **4.3.5. Unauthorized Access:**
  + Accessing data or systems without authorization.
  + Attempting to gain access to another user’s account or files.
* **4.3.6. Data Breaches:**
  + Intentionally or negligently causing a data breach.
  + Failing to report a suspected data breach or security incident.
* **4.3.7. Excessive Personal Use:**
  + Using company resources for personal activities that interfere with work, consume excessive bandwidth, or create security risks. This includes, but not limited to:
  + Excessive streaming, gaming, or social media.
  + Running a personal business.
  + Downloading large, non-work-related files.
* **4.3.8. Inappropriate Content:**
  + Accessing, storing, or distributing inappropriate content, including:
    - Pornography.
    - Hate speech.
    - Content promoting violence or illegal activities.
* **4.3.9. Copyright Infringement**
  + Downloading or sharing copyrighted materials without proper authorization.
* **4.3.10. Unauthorized Modifications:**
  + Making unauthorized changes to system configurations, software, or hardware.

### 4.4. Email and Communication

* Company email accounts are primarily for business use.
* Use professional language and etiquette in all communications.
* Do not send confidential information via email unless it is encrypted.
* Be cautious of phishing emails and suspicious attachments. Do not open attachments or click links from unknown senders.
* Do not use company email for personal advertising, solicitations, or chain letters.

### 4.5. Internet Use

* Internet access is provided for work-related purposes.
* Avoid accessing websites that are known to be risky or contain inappropriate content.
* Be mindful of bandwidth usage.
* Do not download or install software from untrusted sources.

### 4.6. Mobile Device Use

* Company-owned mobile devices must be password-protected.
* Follow company security policies when using mobile devices.
* Report lost or stolen devices immediately.
* Adhere to the Remote Work & BYOD Policy if using a personal device for work.

### 4.7. Social Media

* Be mindful that your online activity, even on personal social media accounts, can reflect on the company.
* Do not disclose confidential company information on social media.
* Do not engage in activities that could damage the company’s reputation.
* Do not represent your personal opinions as those of the company.

## 5. Monitoring

[Company Name] reserves the right to monitor the use of its IT resources, including email, internet activity, file access, and device usage. This monitoring may be conducted without prior notice to ensure compliance with this policy and to protect the security of company systems and data.

## 6. Reporting

Users are required to report any suspected violations of this policy, security incidents, or vulnerabilities to [Designated Contact Person/Department - e.g., Office Manager, IT Support, Owner].

## 7. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

## 8. Revision History

| Version | Date | Author | Description of Change |
| --- | --- | --- | --- |
| 1.0 | March 7, 2025 | Shijie Yin | Initial Policy Creation |