Acceptable Use Policy (AUP) 2026

Organization: [Company Name]

Version: 2026.1

Effective Date: January 1, 2026

1. Purpose

The purpose of this policy is to outline the acceptable use of technology, network resources, and data at [Company Name]. These rules are in place to protect the employee and [Company Name] from illegal or damaging actions by individuals, either knowingly or unknowingly.

2. Scope

This policy applies to all employees, contractors, and third parties who access [Company Name]'s information systems and data.

3. Generative AI & Large Language Models (LLMs)

The use of AI tools (e.g., ChatGPT, Claude, Gemini) is permitted under the following conditions:

- **Data Sovereignty:** Users are strictly prohibited from entering proprietary code, trade secrets, or Personally Identifiable Information (PII) of clients or employees into any public AI tool.
- **Human Oversight:** All AI-generated output must be reviewed by a human for accuracy and bias before being used in business decisions or client-facing materials.
- **Account Usage:** Employees must use company-approved enterprise AI accounts where data "opt-out" for model training is enforced.

4. Remote Work & Connectivity

- **Secure Networks:** Employees must use a company-approved VPN when accessing internal resources from a remote location. Use of public Wi-Fi without a VPN is prohibited.
- **Physical Security:** When working remotely, devices must never be left unattended in public spaces. Screens must be locked when not in use.

5. Personal Device (BYOD) Protocols

If an employee uses a personal device for business purposes:

- **Security Baseline:** The device must have a current operating system, an active screen lock (PIN, Biometric), and full-disk encryption enabled.
- **Right to Wipe:** In the event of device theft or employment termination, [Company Name] reserves the right to remotely wipe business-related data and applications.
- **No Rooting/Jailbreaking:** Accessing company data from "rooted" or "jailbroken" devices is strictly forbidden.

6. Prohibited Activities

- Unauthorized access to data or accounts.
- Circumventing user authentication or security of any host, network, or account.
- Engaging in any activity that is illegal under local or international law.

7. Reporting & Compliance

Any known or suspected violations of this policy must be reported immediately to the Security Officer. Failure to comply may result in disciplinary action, up to and including termination.