[Company Name]
Acceptable Use Policy (AUP)

1. Purpose & Scope

To ensure the security of **[Company Name]** ***(the "Company")*** data and technology assets. This policy applies to all computers, software, BYOD, and networks managed by ***[Company Name] (the "Firm")***.

2. No Expectation of Privacy & BYOD Standards

Employees should have no expectation of privacy when using company-issued devices, BYOD (Bring Your Own Devices) or the company network.

- **Active Monitoring:** The *Company* reserves the right to monitor, log, and review all activity—including internet history, emails, and file transfers—using monitoring software to ensure compliance with *company policies and applicable industry* regulations.
- **BYOD Mandate:** Any personal device utilized for company business (BYOD) is strictly required to have the *Firm's* approved management and security software installed prior to accessing company networks or data. *If an employee declines to install this software, they forfeit the right to access company systems via their personal device.*

3. Prohibited Activities & Web Content Standards

To protect our *business operations, intellectual property,* and client data, the following are strictly prohibited:

- **Malicious & Explicit Content:** Accessing, viewing, downloading, or distributing illegal, sexually explicit, pirated, or malicious content. This policy serves as a strict behavioral deterrent; users are fully accountable for web traffic generated under their credentials to protect both clients and the *Company* from cyber liability.
- **Unapproved Software:** Installing any software, games, or browser extensions without prior approval from the *Firm*.
- **Credential Sharing:** Sharing passwords or allowing others (including family members) to use your company login.

4. Device Updates & Patch Management Maintaining a secure perimeter requires active participation from all end-users to prevent vulnerability exploitation:

- **RMM Compliance:** Employees must promptly accept and execute any system update reminders triggered by the *Firm's* software pop-ups.
- **OS Patching:** Users are required to regularly run normal Windows/OS updates as they become available to ensure the device remains compliant with baseline security standards.

5. Data Storage & Shadow IT

- **Local Storage Restriction:** Saving sensitive company and client data to *local drives (e.g.,* “C:\ drive”, "Desktop" or "Documents" folder) is prohibited. All data must be saved to the designated secure server/drive.
- **Shadow IT Prohibition:** Using personal cloud storage (Dropbox, Google Drive, iCloud, OneDrive) to store or transfer company files is strictly prohibited.

6. Email & Phishing Security

- Never open attachments or click links from unknown senders.
- Never send PII (Personal Identifiable Information) via email unless it is encrypted using the approved secure file transfer tool.
- Report any suspicious emails immediately to the *Firm*.

7. Clean Desk & Physical Security Policy To maintain a secure working environment and protect client data, all employees must adhere to the following Clean Desk requirements:

- **Secure Documents:** All physical documents containing Client PII (e.g., SSNs, birth dates) or proprietary company information must be stored in a locked drawer or cabinet when the employee is away from their desk, especially at the end of the workday.
- **Clear Workspaces:** Desks should be cleared of all sensitive physical materials when not in use. This includes client files, sticky notes with passwords, and printed reports.
- **Lock Screens:** Employees must lock their computer screens (Ctrl+Alt+Del or equivalent) when leaving their workstation unattended for any period of time.
- **Secure Storage:** All confidential electronic media (USB drives, external hard drives) must be stored in a locked container when not actively being used or transferred.

8. Disciplinary Action & Enforcement Escalation Violations of this Acceptable Use Policy represent a direct threat to the *Company’s* operational security and legal standing. Documented infractions will trigger the following codified escalation path:

1. **First Offense:** Formal written warning.
2. **Second Offense:** Second formal warning & meeting with Owner/CEO.
3. **Third Offense:** Immediate loss of network and system access.
4. **Final Action:** Recommendation for employment termination.

Employee Signature: _____

Date: _____