|  |
| --- |
| **Acceptable Use Policy**: InstructionsThe following template is provided for your use and that of your company. This policy should be customized to reflect your environment, and not used AS-IS. 1. Replace [COMPANY LEGAL NAME] with the full legal name of your business
2. Replace [COMPANY NAME] with a shortened name (e.g. ACME instead of ACME Enterprises, LLC)
3. This is a generic policy, but will generally cover most small/medium businesses. Customize to fit your needs.
4. Try to keep this to a single page.
5. Perform full review with legal guidance, as desired
6. Ensure all employees read and sign this annually.
 |

Acceptable Use Policy

# Purpose

The purpose of an Acceptable Use Policy (AUP) is to set expectations of appropriate computer use at [Company Legal Name] ([Company Name]). This policy is not intended to impose any restrictions that are contrary to the productivity of [Company Name]. Rather, this AUP is an agreement between [Company Name], it’s employees, and partners, to protect the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

# Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at [Company Name], including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by [Company Name].

# Policy Provisions

**Due Care.** You are responsible for exercising good judgment regarding appropriate use of [Company Name] resources in accordance with [Company Name] policies, standards, and guidelines. [Company Name] resources may not be used for any unlawful or prohibited purpose.

**Monitoring.** For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the [Company Name] network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

**Password Security.** You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

**Physical Security.** You are responsible for ensuring the protection of assigned [Company Name] assets that includes the use of computer cable locks and other security devices. Computers and any data storage devices must be secured at all times when they are taken from the facility. Promptly report any theft of [Company Name] assets to the [Name of appropriate group].

**Network Access.** Devices that connect to the [Company Name] network must comply with the Minimum Standards Policy and be approved PRIOR to connection.

**Personal Devices.** Personal hardware may be connected to Guest networks. [Company Name] takes no responsibility for the security of these devices. However, all monitoring and access provisions still apply in this policy.

**Circumventing Security.** Do not interfere with corporate device management or security system software, including, but not limited to, antivirus and firewalls.

**Prohibited Network Activities.** [Company Name] networks must not be used to (1) cause a breach or outage on any network, whether under the control of [Company Name] or not; (2) violate any law, including copyright law; (3) intentionally introducing malware to the internal network or the Internet; (4) any scanning activity, unless approved by security in advance.

**Prohibited Communications Activities.** [Company Name] information systems must not be used for (1) supporting illegal activities, and procuring or transmitting material that violates [Company Name] policies against harassment or the safeguarding of confidential or proprietary information; (2) sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication; (3) forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender; (4) use of a [Company Name] e-mail or IP address to engage in conduct that violates [Company Name] policies or guidelines.

# Policy Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name Employee Signature Date