Acceptable Use Policy Template

trio

1. Purpose and Scope

1.1 Purpose:
This Acceptable Use Policy (AUP) aims to establish guidelines for the appropriate use of _____[Company Name]'s IT resources. This policy seeks to protect these resources' confidentiality, integrity, and availability, ensure a productive work environment, and comply with legal and regulatory requirements.

1.2 Scope:
This policy applies to all users accessing _____[Company Name]'s IT resources, including but not limited to employees, contractors, temporary staff, consultants, affiliates, and third-party partners. The IT resources covered by this policy include computers, networks, email systems, internet access, and any other electronic devices or services provided by _____[Company Name].

2. Definitions

2.1 IT Resources:
All hardware, software, networks, and internet services owned or operated by _____[Company Name].

2.2 Users:
Any individual who accesses or uses _____[Company Name]'s IT resources, including employees, contractors, visitors, and other authorized personnel.

2.3 Unacceptable Use:
Any activity that violates this policy, legal regulations, or ethical standards, including but not limited to illegal activities, accessing inappropriate content, or compromising network security.

2.4 Network Security:
Measures implemented to protect IT resources from unauthorized access, misuse, and other security threats.

3. General Use and Ownership

3.1 Ownership:
_____[Company Name]'s IT resources are company-owned and intended primarily for business use. Personal use is permissible as long as it does not interfere with company operations or productivity.

3.2 Monitoring:
_____[Company Name] reserves the right to monitor and access all user activity on its IT resources to ensure compliance with this policy, protect the integrity of its systems, and safeguard sensitive information.

4. Acceptable Use

4.1 Professional Use:
Users must use _____[Company Name]'s IT resources for business-related purposes only, adhering to professional and ethical standards. Acceptable uses include, but are not limited to:
Conducting company business and communications.
Researching topics relevant to job duties.
Accessing company-provided training and development resources.

5. Unacceptable Use

5.1 Prohibited Activities:
The following behaviors and activities are strictly prohibited:

- Illegal Activities: Engaging in activities violating local, state, or federal laws.
- Inappropriate Content: Accessing, uploading, or distributing offensive, threatening, or harmful content.
- Unauthorized Software: Downloading, installing, or using software not approved by the IT department.
- Security Breaches: Attempting to access data or accounts for which the user is not authorized.
- Network Compromise: Introducing malicious software or performing actions that compromise the security or performance of IT resources.

6. Internet and Email Use

6.1 Internet Use:
Users must use the internet in a manner consistent with professional conduct. Personal use is allowed within reasonable limits, provided it does not interfere with work responsibilities or violate this policy.

6.2 Email Use:
Users must use email systems responsibly, maintaining professionalism in all communications. Prohibited activities include:

- Sending unsolicited emails or spam.
- Engaging in harassment via email or other communication channels.
- Sharing sensitive information without proper authorization.

7. Security and Monitoring

7.1 Security Measures:
_____[Company Name] has implemented security measures to protect IT resources and user data. Users are expected to comply with these measures, including:

- Using strong passwords and changing them regularly.
- Reporting any security incidents or potential threats immediately.
- Not sharing login credentials with unauthorized individuals.

7.2 Monitoring Rights:
_____[Company Name] reserves the right to monitor user activities on its IT resources to ensure compliance with this policy and protect the organization's assets and reputation.

8. Consequences of Violations

8.1 Disciplinary Actions:
Violations of this Acceptable Use Policy may result in disciplinary actions, including but not limited to:

- Verbal or written warnings.
- Suspension of access to IT resources.
- Termination of employment or contract.
- Potential legal action.

9. Acknowledgment

9.1 User Acknowledgment:
By accessing _____[Company Name]'s IT resources, users acknowledge that they have read, understood, and agree to comply with this Acceptable Use Policy. Users must sign and return the acknowledgment form to the IT department.

Acknowledgment Form

I, _____[User's Name], have read and understood _____[Company Name]'s Acceptable Use Policy. I agree to comply with the guidelines and standards outlined in this policy.
Signature: _____
Date: _____

This Acceptable Use Policy template can be customized to fit your organization's specific needs and objectives. Regularly review and update this policy to ensure it remains effective and aligned with technological advancements and regulatory changes.

Approval and Revision History
Approved by: _____ **[Name/Title]**
Date: _____ **[Date]**
Next Review Date: _____**[Date]**

Revision History:
Version: _____**[Version Number]**
Changes: _____**[Summary of Changes]**
Date: _____ **[Date]**