Document Name: [COMPANY] Acceptable Use Policy
Last Revision: [INSERT]
Next Revision: [INSERT]
Document Owner: [INSERT TEAM(S)]

[COMPANY] Acceptable Use Policy

Version 1.0

CONFIDENTIAL

Table of Contents

Introduction

At [COMPANY], we provide employees, contractors, and other authorized users with access to company-owned resources such as computers, networks, email systems, and software tools. This Acceptable Use Policy outlines how these resources should be used responsibly, securely, and in a manner that aligns with our business objectives. The goal is to protect both the company and its employees from misuse that could lead to security risks, legal issues, or productivity loss.

Objectives

The purpose of this Acceptable Use Policy is to:

- Set clear expectations for the responsible use of [COMPANY] resources.
- Ensure that our IT infrastructure is used in a way that supports business operations and security.
- Protect the company from illegal activities, security breaches, and inappropriate behavior.
- Promote a culture of respect and integrity in how company resources are used.

Scope

This policy applies to:

- All employees, contractors, vendors, and other individuals who have access to [COMPANY] systems, networks, or devices.
- All company-owned IT resources, including (but not limited to) computers, mobile devices, networks, email accounts, internet access, and software.

This policy applies whether these resources are used on company premises or remotely, including at home or while traveling.

Acceptable Use of Company Resources

At [COMPANY], we expect all users to use our IT resources in a responsible, professional manner. Acceptable uses of these resources include:

- **Work-Related Activities:** Employees must use company resources primarily for performing their job duties, such as sending emails, creating documents, and accessing internal systems.
- **Accessing Company Systems:** Employees may access company systems, databases, and tools only for authorized purposes and as required by their job role.

- **Security Best Practices:** Users must follow all security guidelines, including using strong passwords, enabling multi-factor authentication (where applicable), and reporting any suspected security incidents to the IT team.
- **Respect for Intellectual Property:** Employees should respect copyright, trademarks, and other intellectual property rights when using company resources. This includes using licensed software and following any usage terms.
- **Appropriate Communication:** Employees must use the company's communication tools, such as email and messaging platforms, professionally and respectfully.

Prohibited Activities

To protect [COMPANY] and its employees, certain activities are strictly prohibited when using company resources:

- **Unauthorized Access:** Employees must not attempt to access systems, data, or resources that they are not authorized to use.
- **Illegal Activities:** It is forbidden to use company resources for illegal activities, including (but not limited to) distributing copyrighted material without permission, conducting fraudulent activities, or engaging in any form of harassment.
- **Inappropriate Content:** Employees must not use company resources to access, distribute, or store inappropriate content, such as obscene, offensive, or discriminatory materials.
- **Personal Commercial Use:** Company resources should not be used for personal business activities or commercial gain unrelated to [COMPANY] operations.
- **Installing Unauthorized Software:** Employees may not install unapproved software or hardware on company devices. This includes downloading unauthorized programs, apps, or plugins that could introduce security vulnerabilities.
- **Bypassing Security Measures:** Employees are prohibited from attempting to bypass or disable security measures such as firewalls, antivirus software, or system access controls.

Personal Use Guidelines

We recognize that employees may occasionally use company resources for personal activities. Limited personal use is allowed, provided that it:

- **Does Not Interfere with Work:** Personal use should not affect job performance or interfere with the employee's responsibilities.
- **Is Infrequent and Limited:** Personal use of company devices and systems (e.g., checking personal email, browsing non-work-related websites) must be infrequent and not excessive.

- **Respects Company Resources:** Personal use must not consume significant amounts of bandwidth, storage, or processing power, and should not expose company systems to security risks.
- **Follows Security Practices:** Even during personal use, employees must follow company security guidelines, such as avoiding untrusted websites and ensuring sensitive company data is not exposed.

Monitoring and Enforcement

To ensure compliance with this policy, [COMPANY] reserves the right to monitor the use of its IT resources. This includes, but is not limited to:

- **Email Monitoring:** Company email accounts may be monitored to ensure appropriate use and detect security threats.
- **Internet Usage:** The company may track and log internet activity to ensure compliance with this policy.
- **Device Monitoring:** Company-owned devices may be subject to monitoring for suspicious or unauthorized activity.

Monitoring will be conducted in accordance with applicable privacy laws and regulations. Employees will be notified of any major changes in monitoring practices.

Consequences of Violations

Violations of this Acceptable Use Policy will result in disciplinary action, which may include:

- A verbal or written warning.
- Suspension of access to company systems or devices.
- Termination of employment or contract.
- Legal action, where applicable.

The severity of the consequence will depend on the nature of the violation and whether it was intentional or accidental.

Appendix A: Revision History

This is a controlled document. This section highlights major and minor changes to the document as it is revised.

Revision	Date	Description	Approved by
1.0		Initial Version	