**Acceptable Use Policy Template**

**1. Introduction**

This Acceptable Use Policy ("AUP") outlines the guidelines for proper use of our company's technology resources, including but not limited to computer systems, networks, software, email, internet access, and any other IT services provided by the company. All employees, contractors, and other authorized users are expected to comply with this policy to ensure the security, integrity, and appropriate use of our technology resources.

**1.1 Purpose**

The purpose of this AUP is to:

Protect the company's technology resources from unauthorized or improper use



Ensure the security and privacy of sensitive information



Maintain a productive and respectful work environment



Comply with relevant laws and regulations



Mitigate potential legal and reputational risks



**1.2 Scope**

This policy applies to all individuals who have been granted access to the company's technology resources, including but not limited to:

Full-time and part-time employees



Temporary workers and interns



Contractors and consultants



Vendors and business partners with authorized access



Remote workers and telecommuters



Acceptable Use Policy Template 1

**2. General Guidelines**

**2.1 Authorized Use**

Company technology resources are to be used primarily for business purposes. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any policies outlined in this document.

**2.2 Prohibited Activities**

The following activities are strictly prohibited:

Engaging in any illegal activities or violating any laws



Accessing, creating, or distributing offensive, obscene, or discriminatory content



Harassing, bullying, or intimidating others



Infringing on intellectual property rights



Unauthorized access or attempts to gain unauthorized access to systems or data



Interfering with or disrupting network services



Using company resources for personal financial gain



Downloading or installing unauthorized software



Sharing confidential information without proper authorization



**3. Email and Communication**

**3.1 Professional Communication**

All communication using company email or messaging systems should be professional and respectful. Users should be aware that their communications may be monitored and can be subject to legal discovery.

**3.2 Email Usage**

Acceptable Use Policy Template 2

When using company email, users must:

Use appropriate language and tone



Avoid sending large attachments unless necessary



Be cautious when opening attachments or clicking links from unknown sources



Properly manage and archive important emails Use encryption when sending sensitive information



**3.3 Social Media**

When using social media, employees should:

Clearly distinguish between personal opinions and company statements



Avoid sharing confidential company information



Respect copyright and intellectual property rights



Adhere to the company's social media policy



**4. Internet Usage**

**4.1 Acceptable Use**

Internet access is provided for business purposes. Limited personal use is allowed, provided it does not interfere with work duties or violate this policy.

**4.2 Prohibited Websites**

Accessing the following types of websites is strictly prohibited:

Pornographic or adult content



Gambling or betting sites



Sites promoting hate, extremism, or discrimination



Sites known to contain malware or viruses



File sharing or torrent sites



Acceptable Use Policy Template 3

**4.3 Streaming and Downloads**

Users should limit streaming of audio or video content to work-related purposes. Large downloads should be approved by the IT department to prevent network congestion.

**5. Security and Privacy**

**5.1 Password Management**

Users are responsible for maintaining strong passwords and must:

Use complex passwords with a combination of upper and lowercase letters, numbers, and symbols



Change passwords regularly (at least every 90 days)



Never share passwords with others



Use multi-factor authentication when available



**5.2 Data Protection**

Users must take appropriate measures to protect sensitive data, including:

Encrypting confidential information when storing or transmitting



Using secure file transfer protocols



Properly disposing of physical documents containing sensitive information



Locking computers when away from the workstation



**5.3 Remote Access**

When accessing company resources remotely, users must:

Use company-approved VPN services



Avoid using public Wi-Fi networks without proper security measures



Ensure personal devices used for work are secured and up-to-date



Report lost or stolen devices immediately



Acceptable Use Policy Template 4

**6. Software and Hardware**

**6.1 Authorized Software**

Only software approved and licensed by the company may be installed on company devices. Users must not install personal or unlicensed software without explicit permission from the IT department.

**6.2 Updates and Patches**

Users are responsible for keeping their devices up-to-date with the latest security patches and updates. Automatic updates should be enabled where possible.

**6.3 Hardware Usage**

Company-provided hardware should be used responsibly. Users must:

Protect devices from physical damage, theft, or loss



Not modify or attempt to repair hardware without authorization



Return all company-owned devices upon termination of employment



**7. Monitoring and Privacy**

**7.1 Company Rights**

The company reserves the right to monitor, access, and review all data created, stored, or transmitted using company technology resources. Users should have no expectation of privacy when using these resources.

**7.2 Personal Devices**

If personal devices are used for work purposes, users must comply with the company's Bring Your Own Device \BYOD\ policy and understand that work-related data on personal devices may be subject to monitoring and review.

**8. Compliance and Enforcement**

Acceptable Use Policy Template 5

**8.1 Reporting Violations**

Users are required to report any suspected violations of this policy to their supervisor or the IT department immediately.

**8.2 Consequences of Violations**

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. In some cases, legal action may be taken.

**8.3 Policy Reviews and Updates**

This policy will be reviewed annually and updated as necessary to reflect changes in technology, laws, or business requirements.

**9. Acknowledgment**

All users must acknowledge that they have read, understood, and agree to comply with this Acceptable Use Policy. By using company technology resources, users implicitly agree to the terms outlined in this policy.

Last updated: @September 16, 2024

For any questions or clarifications regarding this Acceptable Use Policy, please contact the IT department or Human Resources.

Acceptable Use Policy Template 6