IT Acceptable Use Policy (AUP)

In today’s rapidly evolving technological landscape, maintaining productivity and protecting IT systems and sensitive data are critical. Employees play a pivotal role in ensuring the security and proper use of IT systems, including adherence to cybersecurity best practices. This Acceptable Use Policy (AUP) establishes the expectations and guidelines for all users accessing IT systems within The Company.

**1. Introduction**

This AUP outlines the acceptable use of IT systems to safeguard The Company, its employees, customers, and partners from harm caused by misuse, whether intentional or accidental.

Consequences of misuse may include data breaches, legal or financial penalties, reputational harm, and productivity loss. Adherence to this policy is mandatory, and employees should seek clarification from their manager or IT security officer if needed.

**2. Definitions**

* **Users**: Individuals with access to The Company’s IT systems, including employees, contractors, consultants, suppliers, and business partners.
* **Systems**: All IT assets connected to The Company’s network, including computers, mobile devices, software, data, cloud platforms, and communication tools.

**3. Scope**

This policy applies universally to all Users and Systems. Specific policies for certain roles or systems may take precedence where they conflict with this document but otherwise must be followed concurrently.

Compliance with local laws and regulations always takes precedence, and any necessary clarifications should be issued locally.

**4. General Use of IT Systems**

* **Ownership**: All data and activities conducted on The Company’s systems are considered the property of The Company.
* **Personal Use**: Limited personal use is permitted as long as it does not interfere with productivity, incur significant costs, or compromise security.
* **Monitoring**: The Company reserves the right to monitor IT systems, including emails, chats, files, and usage history, within the boundaries of applicable laws.

**5. Data Security**

* **Classification**: Sensitive or confidential data must be clearly marked and handled with appropriate security measures, including encryption.
* **Access Control**: Only authorized personnel should access confidential data, and sharing sensitive information must be explicitly approved.
* **Password Management**: Users must use strong, unique passwords and never share their credentials.
* **Device Security**: Portable devices must be secured with encryption and lock-on-idle after 10 minutes of inactivity. Users are responsible for the security of devices issued to them.
* **Malware Protection**: Users must avoid introducing malware by practicing safe browsing and promptly reporting any suspected infections.

**6. AI Use and Privacy**

* **AI Tools**: Users may use approved AI tools to enhance productivity, but any AI-generated output involving sensitive or confidential company data must be reviewed for accuracy and security.
* **Privacy Concerns**: Employees must not upload proprietary or personal information to public AI platforms or tools without explicit approval.
* **Ethical Use**: AI tools must not be used to create misleading content, infringe on intellectual property, or breach data privacy regulations.

**7. Cybersecurity Awareness**

* **Training**: Users are required to complete regular cybersecurity training to recognize phishing, social engineering, and other cyber threats.
* **Incident Reporting**: Any suspected security incidents, such as phishing emails, unauthorized access, or malware, must be reported immediately.
* **Updates**: Users must keep their systems and software updated with the latest security patches.

**8. Unacceptable Use**

Users must avoid any activities that:

* Violate laws, regulations, or company policies.
* Infringe on intellectual property or data privacy.
* Compromise security, such as sharing passwords or disabling security features.
* Damage The Company’s reputation or disrupt operations, including accessing inappropriate content or engaging in hate speech, harassment, or gambling.
* Circumvent established IT security systems or protocols.

**9. Enforcement**

Violations of this policy will result in disciplinary action, up to and including termination of employment. Illegal activities may lead to immediate dismissal and will be reported to law enforcement.

**10. Acknowledgment**

All users must acknowledge they have read, understood, and agree to comply with this policy. Any questions or concerns should be directed to the IT department or a designated manager.

This policy will be reviewed regularly to ensure it remains current with evolving technologies and threats.

**11. Acceptance**

All users must acknowledge they have read, understood, and agree to comply with this policy. Any questions or concerns should be directed to the IT department or a designated manager.

This policy will be reviewed regularly to ensure it remains current with evolving technologies and threats.

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_