US Solutions Pvt Ltd. - Acceptable Use Policy (AUP)

1. Introduction

This Acceptable Use Policy (AUP) outlines the guidelines and expectations for the use of US Solutions Pvt Ltd. ("the Company") information technology (IT) resources, including but not limited to computers, laptops, mobile devices, networks, internet access, email, software, and data. This policy aims to ensure the security, integrity, and availability of our IT infrastructure, protect confidential information, and maintain a professional and productive work environment. All employees, contractors, and temporary staff ("Users") are required to read, understand, and comply with this policy.

2. Purpose

The purpose of this AUP is to:

- Define acceptable and unacceptable uses of Company IT resources.
- Protect the Company's intellectual property, confidential data, and reputation.
- Ensure compliance with applicable laws and regulations.
- Maintain the security and integrity of the Company's IT infrastructure.
- Promote efficient and responsible use of IT resources.
- Establish clear consequences for policy violations.

3. Scope

This policy applies to all Users who access or use any Company IT resources, regardless of location or device. This includes, but is not limited to:

- Company-owned or leased computers, laptops, tablets, and mobile devices.
- Company networks, including wired and wireless connections.
- Company email and messaging systems.
- Company software and applications.
- Company data and information, regardless of storage location.
- Internet access provided by the Company.
- Personal devices used to access Company resources (BYOD).

4. General Principles

- **Authorized Use Only:** Users are authorized to use Company IT resources solely for legitimate business purposes.
- **Confidentiality and Security:** Users must protect the confidentiality and security of Company data and information.
- **Compliance:** Users must comply with all applicable laws, regulations, and Company policies.
- **Professional Conduct:** Users must maintain a professional and respectful demeanor when using Company IT resources.
- **No Expectation of Privacy:** Users should have no expectation of privacy when using Company IT resources. The Company reserves the right to monitor and access all data and communications.

5. Specific Guidelines

5.1. Computer and Device Usage:

- Users must use assigned computers and devices responsibly and in accordance with Company guidelines.
- Users must not install unauthorized software or hardware on Company devices.
- Users must protect Company devices from physical damage, theft, and unauthorized access.
- Users must log off or lock their computers when unattended.
- Users are responsible for ensuring operating systems and software patches are kept up to date when prompted by the system.
- BYOD devices must comply with minimum security requirements as set by the IT department.

5.2. Network and Internet Usage:

- Users must use Company networks and internet access for legitimate business purposes only.
- Users must not engage in illegal or unethical activities, such as hacking, phishing, or distributing malware.
- Users must not download or distribute copyrighted materials without proper authorization.
- Users must not use Company networks for personal gain or commercial activities.
- Excessive bandwidth usage for non-work related activities is prohibited.
- Use of VPNs on company owned devices for non work related activity is strictly prohibited.

5.3. Email and Messaging:

- Users must use Company email and messaging systems for professional communication only.
- Users must not send or forward inappropriate or offensive content.
- Users must not send unsolicited emails or spam.
- Users must protect Company email accounts from unauthorized access.
- Users must adhere to the companies data retention policies related to email.
- Users must understand that any email sent from their company email address is considered a representation of the company.

5.4. Software and Data:

- Users must use Company software and applications in accordance with licensing agreements.
- Users must not copy or distribute Company software without authorization.
- Users must protect Company data from unauthorized access, modification, or destruction.
- Users must not store personal data on Company systems without authorization.
- Users must adhere to the company's data classification policy.
- Users must back up data as required by the company’s backup policy.

5.5. Social Media:

- Users must represent the Company professionally on social media platforms.
- Users must not disclose confidential Company information on social media.
- Users must not post defamatory or offensive content about the Company, its employees, or clients.
- Users must adhere to the Company's social media policy.
- Users must disclose their affiliation with the company when discussing company related topics on social media.

5.6. Security:

- Users must use strong passwords and change them regularly.
- Users must not share passwords or other authentication credentials.
- Users must report any security incidents or suspected security breaches immediately to the IT department.
- Users must not attempt to bypass security controls or access unauthorized systems.
- Users must not disable or tamper with security software.
- Users must be aware of and report phishing attempts.

6. Monitoring and Enforcement

The Company reserves the right to monitor and access all User activity on Company IT resources. This includes, but is not limited to, email, internet usage, file access, and system logs. The Company may use this information to investigate suspected policy violations, ensure compliance, and protect its interests.

Violations of this AUP may result in disciplinary action, up to and including termination of employment or contract. The Company may also take legal action to protect its rights and interests.

7. Policy Review and Updates

This AUP will be reviewed and updated periodically to reflect changes in technology, regulations, and Company policies. Users are responsible for staying informed about any updates to this policy.

8. Acknowledgement

By accessing or using Company IT resources, Users acknowledge that they have read, understood, and agree to comply with this AUP.

9. Incident Reporting

Any suspected or actual security incident or policy violation must be immediately reported to the IT department or the security team.

10. Data Classification.

All data at US Solutions Pvt Ltd. will be classified into the following 3 categories.

- **Public:** Data that is meant to be shared with the public.
- **Internal:** Data that is for internal use only.
- **Confidential:** Data that is extremely sensitive and needs to be protected.

Each data type will have specific handling and security requirements.

11. Password Policy.

All passwords must adhere to the following.

- Minimum 12 characters.
- Mixture of upper and lower case letters.
- At least one number.
- At least one special character.
- Passwords must be changed every 90 days.
- Password reuse is prohibited.
- Passwords must not be stored in plain text.
- Multi factor authentication must be used when possible.

12. Mobile Device Usage.

- Mobile devices used for company work must be protected by a strong password or biometric authentication.
- Mobile devices must be kept up to date with the latest security patches.
- Mobile devices must be configured to remotely wipe data if lost or stolen.
- Sensitive company data must be encrypted on mobile devices.
- Unauthorized software installation is prohibited.
- Users must report lost or stolen devices immediately.

13. Remote access.

- Remote access to the company network must be done using a company approved VPN.
- Remote access must be protected by multi factor authentication.
- Remote access must only be used for business purposes.
- Users must not leave remote access sessions unattended.
- Users must ensure that their home network is secure.

14. Legal Compliance.

Users must adhere to all local, national and international laws. This includes but is not limited to data privacy laws, intellectual property laws, and export control laws.

This AUP is designed to protect the Company's IT resources and ensure a safe and productive work environment. By adhering to these guidelines, Users contribute to the overall security and success of US Solutions Pvt Ltd.