US Solutions Pvt Ltd. - Information Security Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-01-26
- **Author:** IT & Infosec Department - Benjamin Carter
- **Approved By:** Eleanor Vance, Chief Information Officer (CIO)
- **Effective Date:** 2024-02-22
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that information is a critical asset and that its protection is essential for maintaining business operations, preserving customer trust, and ensuring compliance with legal and regulatory requirements. This Information Security Policy establishes the overarching framework for protecting all information assets within the Company. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a comprehensive information security framework.
- Protect the confidentiality, integrity, and availability of Company information assets.
- Minimize the risk of security incidents and data breaches.
- Ensure compliance with applicable laws, regulations, and industry standards.
- Define the responsibilities of all Users regarding information security.

3. Scope

This policy applies to all information assets owned, processed, or managed by US Solutions Pvt Ltd., including:

- Electronic data (e.g., databases, documents, emails).
- Physical data (e.g., paper documents, hard drives).
- Software and applications.
- Network infrastructure and devices.
- Cloud-based services.
- All information, regardless of storage or transmission medium.

4. Information Security Principles

The following principles guide our information security practices:

- **Confidentiality:** Information should be accessible only to authorized individuals.
- **Integrity:** Information should be accurate and complete, and protected from unauthorized modification.
- **Availability:** Information should be accessible to authorized users when needed.

- **Accountability:** Users are responsible for their actions related to information security.
- **Non-Repudiation:** Actions related to information should be traceable to the responsible party.
- **Risk Management:** Information security risks should be identified, assessed, and mitigated.
- **Compliance:** Information security practices should comply with all applicable laws and regulations.

5. Information Security Responsibilities

- **Management:**
  - Establish and maintain an effective information security program.
  - Provide resources and support for information security initiatives.
  - Ensure compliance with this policy.
- **IT & Infosec Department:**
  - Implement and maintain security controls and technologies.
  - Monitor and respond to security incidents.
  - Conduct security assessments and audits.
  - Provide security awareness training.
- **Data Owners:**
  - Classify data based on its sensitivity and criticality.
  - Determine access requirements for their data.
  - Ensure data is handled in accordance with this policy.
- **All Users:**
  - Comply with this Information Security Policy and related procedures.
  - Protect Company information from unauthorized access and disclosure.
  - Report any suspected security incidents or vulnerabilities.
  - Attend security awareness training.

6. Information Security Controls

The Company implements various security controls to protect information assets, including:

- **Access Control:** Implementing least privilege and need-to-know access.
- **Authentication:** Using strong passwords and multi-factor authentication (MFA).
- **Encryption:** Encrypting sensitive data at rest and in transit.
- **Network Security:** Implementing firewalls, intrusion detection systems, and VPNs.
- **Malware Protection:** Using antivirus and anti-malware software.
- **Patch Management:** Regularly patching systems and applications.
- **Data Backup and Recovery:** Implementing regular data backups and disaster recovery plans.
- **Incident Response:** Establishing procedures for handling security incidents.
- **Security Awareness Training:** Providing regular training to Users.
- **Physical Security:** Controlling physical access to Company facilities.

7. Data Classification

- All information assets must be classified according to the Company's Data Classification Policy.
- Classification levels (e.g., Public, Internal, Confidential, Restricted) determine the appropriate security controls.

8. Risk Management

- The Company conducts regular risk assessments to identify and evaluate information security risks.
- Risk mitigation strategies are implemented to reduce the likelihood and impact of security incidents.

9. Legal and Regulatory Compliance

- The Company complies with all applicable laws, regulations, and industry standards, including but not limited to:
    - General Data Protection Regulation (GDPR).
    - California Consumer Privacy Act (CCPA).
    - Payment Card Industry Data Security Standard (PCI DSS).[1]
- Compliance is regularly monitored and audited.

10. Security Awareness Training

- All Users are required to complete security awareness training upon hire and annually thereafter.
- Training covers topics such as password security, phishing awareness, and data handling.

11. Incident Reporting

- Users must immediately report any suspected security incidents to the IT & Infosec Department ([email address removed]).
- The Incident Response Team (IRT) will investigate and respond to incidents according to the Incident Response Policy.

12. Policy Review and Updates

- This Information Security Policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

13. Acknowledgement

- By accessing Company information assets, Users acknowledge that they have read, understood, and agree to comply with this Information Security Policy.

This Information Security Policy is designed to protect US Solutions Pvt Ltd.'s information assets and maintain a secure and compliant work environment. By adhering to these guidelines, Users contribute to the overall security and success of the Company.