US Solutions Pvt Ltd. - Third-Party/Vendor Security Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-02-23
- **Author:** IT & Infosec Department - Richard Holt
- **Approved By:** Valerie Sinclair, Vendor Management Director
- **Effective Date:** 2024-03-22
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. engages with various third-party vendors and service providers to support our business operations. These partnerships introduce potential security risks that must be managed effectively. This Third-Party/Vendor Security Policy outlines the guidelines and procedures for assessing, managing, and mitigating security risks associated with third-party relationships. All employees and vendors are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a standardized approach to third-party/vendor security.
- Protect Company data and systems from security risks associated with third-party access.
- Ensure that vendors comply with applicable laws, regulations, and industry standards.
- Define the responsibilities of the Company and vendors regarding security.
- Minimize the risk of data breaches and security incidents.

3. Scope

This policy applies to all third-party vendors and service providers who:

- Access Company systems or data.
- Process, store, or transmit Company data.
- Provide services that impact the security of Company operations.
- Any relationship where US Solutions Pvt Ltd. shares information with a third party.

4. Vendor Security Requirements

- **Security Assessments:**
    - Vendors must undergo security assessments before being granted access to Company systems or data.
    - Assessments may include questionnaires, on-site audits, and vulnerability scans.

    - The IT & Infosec department will review and approve vendor security assessments.
- **Security Controls:**
    - Vendors must implement appropriate security controls to protect Company data and systems.
    - Controls may include access controls, encryption, network security, and incident response procedures.
    - Vendors must adhere to the security requirements outlined in contracts and service level agreements (SLAs).
- **Data Protection:**
    - Vendors must comply with all applicable data privacy laws and regulations (e.g., GDPR, CCPA).
    - Vendors must protect Company data from unauthorized access, loss, or disclosure.
    - Vendors must notify the Company of any data breaches or security incidents.
- **Incident Response:**
    - Vendors must have an incident response plan in place to address security incidents.
    - Vendors must notify the Company of any security incidents that may impact Company operations.
    - Vendors must cooperate with the Company during incident response activities.
- **Background Checks:**
    - For vendors that have access to sensitive data, background checks may be required for vendor personnel.

5. Vendor Management Process

- **Vendor Selection:**
    - Security considerations must be included in the vendor selection process.
    - Vendors must be evaluated based on their security capabilities and track record.
- **Contracts and SLAs:**
    - Contracts and SLAs must include security requirements and responsibilities.
    - Contracts must address data ownership, access control, and incident response procedures.
    - Contracts must include right to audit clauses.
- **Vendor Monitoring:**
    - Vendors must be monitored regularly to ensure compliance with security requirements.
    - Monitoring may include periodic security assessments, audits, and performance reviews.
    - The Vendor Management team will conduct periodic reviews.
- **Offboarding:**
    - Vendor access must be revoked promptly upon termination of the relationship.
    - Vendor data must be securely returned or destroyed.
    - Confirmation of data destruction must be provided.

6. Company Responsibilities

- **Vendor Security Assessment:**
  - The IT & Infosec department is responsible for conducting vendor security assessments.
- **Contract Management:**
  - The Legal and Vendor Management departments are responsible for including security requirements in contracts and SLAs.
- **Vendor Monitoring:**
  - The Vendor Management team is responsible for monitoring vendor compliance.
- **Incident Response:**
  - The IT & Infosec department is responsible for coordinating incident response activities with vendors.
- **Communication:**
  - Maintain clear communication channels with vendors regarding security.

7. Vendor Responsibilities

- **Compliance:**
  - Vendors must comply with all applicable laws, regulations, and Company policies.
- **Security Controls:**
  - Vendors must implement and maintain appropriate security controls.
- **Notification:**
  - Vendors must notify the Company of any security incidents or data breaches.
- **Cooperation:**
  - Vendors must cooperate with the Company during security assessments and incident response activities.

8. Legal and Regulatory Compliance

- This policy complies with all applicable data privacy laws and regulations (e.g., GDPR, CCPA).
- Vendor security practices must be consistent with legal and regulatory requirements.

9. Training and Awareness

- Employees involved in vendor management will receive training on this policy.
- Vendors will be provided with information about Company security requirements.

10. Policy Review and Updates

- This 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 employees and vendors.

11. Monitoring and Enforcement

- The Vendor Management team will monitor vendor compliance and enforce this policy.
- Violations of this policy may result in termination of the vendor relationship.

12. Acknowledgement

- By engaging with US Solutions Pvt Ltd., vendors acknowledge that they have read, understood, and agree to comply with this Third-Party/Vendor Security Policy.

This Third-Party/Vendor Security Policy is designed to protect US Solutions Pvt Ltd.'s data and systems from security risks associated with vendor relationships. By adhering to these guidelines, employees and vendors contribute to a secure and compliant business environment.