US Solutions Pvt Ltd. - Data Classification Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2023-12-22
- **Author:** IT & Infosec Department - Jessica Patel
- **Approved By:** Thomas O'Connell, Chief Information Security Officer (CISO)
- **Effective Date:** 2024-01-15
- **Review Frequency:** Annually

1. Introduction

The protection of information assets is critical to the success of US Solutions Pvt Ltd. This Data Classification Policy establishes a framework for categorizing data based on its sensitivity and criticality. Proper classification ensures that appropriate security controls are applied to protect information from unauthorized access, modification, or destruction. 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 consistent data classification system.
- Ensure that sensitive information is adequately protected.
- Facilitate compliance with applicable laws and regulations.
- Define the responsibilities of data owners and custodians.
- Minimize the risk of data breaches and unauthorized disclosure.

3. Scope

This policy applies to all data created, processed, stored, or transmitted by US Solutions Pvt Ltd., regardless of the format or medium. This includes:

- Electronic data (e.g., documents, databases, emails).
- Physical data (e.g., paper documents, hard drives).
- Verbal communications.

4. Data Classification Levels

Data is classified into the following levels:

- **Public (Level 1):**
    - Information that is intended for public disclosure and has minimal impact on the Company if disclosed.
    - Examples: Marketing materials, public website content, press releases.
    - Security Requirements: Basic access controls, public availability.
- **Internal (Level 2):**
    - Information that is intended for internal use only and could have a moderate impact on the Company if disclosed without authorization.

    - Examples: Internal policies, employee handbooks, non-sensitive project documents.
    - Security Requirements: Access controls limited to authorized employees, secure storage within the company network.
- **Confidential (Level 3):**
    - Information that is highly sensitive and could have a significant impact on the Company if disclosed without authorization.
    - Examples: Financial data, client contracts, intellectual property, employee personal data.
    - Security Requirements: Strict access controls, encryption, secure storage, limited distribution.
- **Restricted (Level 4):**
    - Information that is extremely sensitive and could have a severe impact on the Company if disclosed without authorization.
    - Examples: Source code, customer credit card data, trade secrets, classified government information.
    - Security Requirements: Strongest access controls, robust encryption, strict need to know basis, audit logging, and monitored access.

5. Data Owner and Custodian Responsibilities

- **Data Owner:**
    - Determines the classification level of data.
    - Approves access to data.
    - Ensures compliance with this policy.
    - Reviews data classifications periodically.
- **Data Custodian:**
    - Implements security controls based on the data classification level.
    - Ensures data integrity and availability.
    - Maintains access logs and audit trails.
    - Informs data owners of security incidents.

6. Data Handling Guidelines

- **Labeling:**
    - All documents and electronic files must be labeled with the appropriate classification level.
    - Email subject lines should indicate the classification level of the content.
- **Storage:**
    - Data must be stored in accordance with its classification level.
    - Confidential and Restricted data must be encrypted when stored.
    - Physical storage must be secured appropriately.
- **Transmission:**
    - Data must be transmitted securely, using encryption or other appropriate methods.
    - Confidential and Restricted data must not be transmitted over unsecured networks.
- **Access Control:**

    - Access to data must be granted on a need-to-know basis.
    - Access controls must be regularly reviewed and updated.
    - Principle of least privilege must be followed.
- **Disposal:**
    - Data must be securely disposed of when no longer needed.
    - Electronic data must be securely wiped or shredded.
    - Physical documents must be shredded or destroyed.

7. Data Classification Process

- Data owners are responsible for classifying their data.
- The IT department provides guidance and support for data classification.
- Data classification should be reviewed and updated periodically.
- Any newly created data must be classified.

8. Legal and Regulatory Compliance

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

9. Training and Awareness

- All Users will receive training on this Data Classification Policy.
- Regular security awareness training will be provided to reinforce data classification best practices.

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 Users.

11. Monitoring and Enforcement

- The IT department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination[1] of employment or contract.

12. Acknowledgement

- By accessing Company data, Users acknowledge that they have read, understood, and agree to comply with this Data Classification Policy.

This Data Classification Policy is designed to protect US Solutions Pvt Ltd.'s information assets and ensure compliance with applicable laws and regulations. By adhering to these guidelines, Users contribute to a secure and compliant work environment.