# Contoso Data Handling Policy

Version 1.0

Effective Date: February 8, 2024

1. Introduction

Contoso is committed to protecting the confidentiality, integrity, and availability of all physical and electronic information assets throughout their lifecycle. This data handling policy outlines the company's approach to handling data, including collection, storage, processing, access, and disposal, to ensure compliance with applicable legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all employees, contractors, and third-party service providers of Contoso who have access to data owned, held, or processed by or on behalf of the company, regardless of the location or medium.

3. Data Classification

Data within Contoso is classified into the following categories:

Public: Data intended for public disclosure.

Internal: Data that is sensitive within the company but is not confidential.

Confidential: Data whose unauthorized disclosure could adversely impact Contoso or its stakeholders.

Regulated: Data subject to specific regulatory compliance requirements.

4. Data Collection and Processing

Contoso collects and processes data solely for legitimate business purposes. The collection of data will be fair, lawful, and limited to the information necessary for the intended purpose. All data processing activities must be approved by the Data Protection Officer (DPO).

5. Data Storage and Transmission

Storage: Data must be stored in a manner that ensures its security, taking into account the classification. Confidential and regulated data should be encrypted at rest.

Transmission: Data must be encrypted during transmission over public networks. The method of encryption will be consistent with current industry standards.

6. Data Access and Disclosure

Access to data within Contoso is based on the principle of least privilege. Employees, contractors, and third-party service providers will have access only to the data necessary for their role. Disclosure of confidential and regulated data outside of Contoso is strictly controlled and must be authorized by the DPO.

7. Data Retention and Disposal

Contoso retains data only for as long as it is necessary for the purposes for which it was collected or as required by law. Data disposal practices will ensure the permanent removal of data when it is no longer needed, using methods that prevent data recovery.

8. Data Security and Breach Response

Security: Contoso implements appropriate physical, technical, and organizational measures to protect data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Breach Response: In the event of a data breach, Contoso has a response plan that includes notification to affected individuals and regulatory authorities as applicable, in accordance with legal and contractual obligations.

9. Training and Awareness

All employees, contractors, and third-party service providers with access to data must complete data protection training upon commencement of their duties and annually thereafter. This training covers data handling practices, responsibilities, and the consequences of policy violations.

10. Policy Review and Updates

This policy will be reviewed annually or in response to significant changes to the business, technology, or data protection legislation. Amendments will be approved by senior management.

11. Compliance and Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contracts. Suspected violations should be reported to the DPO immediately.

Data Protection Officer Contact Information:

Name: Jane Doe

Email: dpo@contoso.com

Phone: +1 (555) 123-4567

This policy is effective as of the date stated at the top of the document. All employees, contractors, and third-party service providers are required to comply with this policy as part of their agreement with Contoso.