Data Classification Policy

Version: 1.0

Owner: Data Governance Team

Effective Date: [Insert Date]

Last Reviewed: [Insert Date]

Purpose:

To establish a classification framework for all company information based on sensitivity and regulatory requirements.

Scope:

Applies to all employees and contractors who handle, access, or store organizational data.

Classification Levels:

1. Confidential

- Includes PII, financial records, health data, or trade secrets.

- Requires encryption, access control, and logging.

2. Internal Use Only

- Includes internal documentation, emails, and operational data.

- Accessible only to employees and trusted third parties.

3. Public

- Includes content approved for public distribution, such as website content or marketing materials.

Handling Guidelines:

- Label documents appropriately (Confidential, Internal, Public).
- Do not email Confidential data without encryption.
- Store all Internal and Confidential data on approved systems.

Enforcement:

Failure to follow handling guidelines may result in disciplinary action or termination.

Review Cycle:

Review annually or when new data categories are introduced.