Data Classification and Handling Policy

This policy defines the classification of organizational data and outlines handling requirements to protect sensitive information.  
The purpose is to ensure data confidentiality, integrity, and availability based on its sensitivity and value.

# 1. Classification Levels

• Public – Data intended for public use (e.g., website content).   
• Internal – Data meant for internal use but not sensitive (e.g., internal memos).   
• Confidential – Sensitive business data (e.g., customer information, financials).   
• Restricted – Highly sensitive data (e.g., credentials, trade secrets, PII).

# 2. Handling Requirements

• Public – May be shared externally with no restriction.   
• Internal – Share only with authorized employees; no external distribution.   
• Confidential – Encrypt during storage and transmission; limit access.   
• Restricted – Encrypted, tightly controlled access, and stored in secure environments only.

# 3. Access Control

• Access to Confidential and Restricted data must be approved by a data owner.   
• Role-based access control (RBAC) must be enforced.

# 4. Storage and Transmission

• Use approved cloud or on-premises platforms.   
• Never transmit Confidential or Restricted data over unsecured channels.

# 5. Disposal

• Data must be securely deleted when no longer needed.   
• Use tools approved by IT for wiping storage media.

# 6. Training and Compliance

• Employees must be trained on data classification annually.   
• Non-compliance may lead to disciplinary action.