Organizational Data Security Policy

1. Purpose

This document establishes the security policy for protecting organizational data assets against loss, unauthorized disclosure, or unauthorized modification.

2. Scope

This policy applies to all employees, contractors, and third parties who access, store, or process organizational data.

3. Policy Statements

3.1 Data Classification

- All data must be classified as Public, Internal, Confidential, or Restricted.
- Data classification determines required protection measures.

3.2 Access Control

- Access to organizational data shall follow the principle of least privilege.
- Authentication and authorization are required for access to Confidential or Restricted data.

3.3 Data Protection

- Encryption must be used for transmitting and storing Sensitive, Confidential, or Restricted data.
- Sensitive data shall not be stored on personal devices without approval.

3.4 Incident Response

- All suspected or actual security incidents must be reported to the Security Team immediately.
- An investigation and response will be initiated as per the Incident Response Procedure.

3.5 Data Retention and Disposal

- Data must be retained only as long as required by law or business need.
- Obsolete data must be disposed of securely to prevent unauthorized access.

4. Roles and Responsibilities

- All users are responsible for complying with this policy.
- The Security Team oversees policy implementation and guidance.
- Management ensures staff are informed and trained as needed.

5. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

6. Review and Revision

This policy shall be reviewed annually and updated as required to reflect changes to organizational needs or legal requirements.