Somalia Data Protection Authority

Compliance Toolkit Template

DATA CLASSIFICATION POLICY

Version: 1.0
Date of Issue: January 2026
Status: Recommended Best Practice (Mandatory for medium and large organizations)
Issued under: Somalia Data Protection Act No. 005 (2023)

1. Purpose

This policy establishes a framework for classifying data according to its sensitivity to ensure appropriate protection and handling of personal data.

This policy supports compliance with the data security and accountability obligations under the Somalia Data Protection Act No. 005 (2023).

2. Scope

This policy applies to all employees, contractors, consultants, and third parties handling data on behalf of **[Organization Name]**.

3. Data Classification Levels

3.1 Public Data

Information approved for public disclosure.

Examples include:

- Public announcements
- Marketing materials

Handling requirements:

- No confidentiality restrictions
- May be freely shared

3.2 Internal Data

Information intended for internal organizational use.

Examples include:

- Internal emails
- Operational procedures

Handling requirements:

- Restricted to authorized personnel
- Stored within approved internal systems

3.3 Confidential Data

Sensitive information requiring protection.

Examples include:

- Personal data
- Employee records
- Customer data

Handling requirements:

- Access limited on a need-to-know basis
- Secure storage and transmission
- Access controls and authentication mechanisms

3.4 Highly Sensitive Data

Data that could cause serious harm if compromised.

Examples include:

- Health data
- Biometric data

- Financial account details
- Children's data

Handling requirements:

- Strict access controls
- Highly Sensitive Data must be encrypted in storage and transmission unless technically infeasible
- Enhanced monitoring and logging
- Data Protection Impact Assessments (DPIAs) where applicable
- Restricted sharing and documented authorization

4. Roles and Responsibilities

- **Management** ensures enforcement and oversight of this policy.
- **Employees and contractors** must classify and handle data appropriately.
- The **Data Protection Officer (if appointed)** oversees compliance and reviews classifications periodically.

Failure to comply with this policy may result in disciplinary action in accordance with internal procedures.

5. Data Handling Rules

All data must be:

- Classified upon creation or collection
- Stored securely according to its classification level
- Transmitted using approved secure methods
- Accessed only by authorized personnel
- Deleted securely at the end of its retention period

6. Breach Management

Any unauthorized access, disclosure, alteration, or misuse of classified data must be reported immediately in accordance with the organization's data breach procedures and the Somalia Data Protection Act.

7. Training and Awareness

Employees must receive regular training on:

- Data classification standards
- Secure handling procedures
- Security and confidentiality obligations

8. Policy Review

This policy shall be reviewed at least annually or following significant organizational, technological, or legal changes.

Approved by: _____
Date: _____
Signature: _____

Disclaimer

This template is provided by the Somalia Data Protection Authority for general guidance purposes. Organizations remain responsible for ensuring compliance with the Somalia Data Protection Act No. 005 (2023). Use of this template does not constitute approval or certification by the DPA.