Somalia Data Protection Authority (DPA)

Official Technical Guidance on Data Security Best Practices

Status: Official Technical Guidance
Version: 1.0
Date of Issue: 2025

Foreword

The Somalia Data Protection Authority (DPA) issues this Technical Guidance to assist controllers and processors in implementing appropriate technical and organizational measures to protect personal data in accordance with Law No. 005 (2023).

Effective data security is fundamental to safeguarding individual rights, maintaining public trust, and supporting secure digital transformation across Somalia.

1.1 Legal Requirement

Organizations must implement appropriate technical and organizational measures to protect personal data against:

- Unauthorized access
- Accidental or unlawful destruction
- Loss, alteration, or disclosure

Security measures must be proportionate to risk, taking into account:

- Nature of data
- Sensitivity
- Scale of processing
- Potential harm to individuals

Security measures must be risk-based and regularly reviewed in light of evolving threats and technological developments.

1.2 Technical Security Measures

Organizations should implement the following minimum technical controls:

Access Control

- Role-based access controls (RBAC)
- Least-privilege principle
- Multi-factor authentication (MFA) for sensitive systems
- Unique user accounts (no shared credentials)

Encryption

- Encryption of personal data at rest
- Encryption of personal data in transit
- Encryption of backups and removable media

Network Security

- Firewalls and intrusion detection systems
- Secure VPNs for remote access
- Network segmentation for sensitive systems

System Hardening

- Regular software updates and patching
- Secure configuration of servers and databases
- Removal of unnecessary services and default credentials

Logging and Monitoring

- Logging of system access and data access
- Monitoring for unauthorized activity
- Retention of logs for audit and investigation purposes

1.3 Organizational Security Measures

Organizations must also implement:

- Written information security policies
- Staff confidentiality obligations
- Mandatory staff training on data security
- Vendor and processor security assessments

- Ongoing monitoring of the security posture of vendors and processors handling personal data
- Secure physical access controls
- Clear incident reporting procedures
- An incident response plan aligned with breach notification obligations under the Act

Organizations must ensure that incident response procedures enable timely containment, assessment, and notification in accordance with statutory timelines.

1.4 Special Protection for Sensitive Data

Sensitive personal data (health, biometric, financial, children's data) requires enhanced safeguards, including:

- Encryption by default
- Strict access limitations
- Additional monitoring
- Data Protection Impact Assessments (DPIAs)
- Enhanced vendor due diligence where sensitive data is shared

1.5 Security Accountability

Organizations must be able to demonstrate security compliance to the DPA through:

- Documented policies
- Audit logs
- Risk assessments
- DPIAs
- Breach records
- Security testing and review documentation

Failure to implement adequate security measures may result in enforcement action under the Act.

Security compliance is an ongoing obligation and must be periodically reviewed and updated.

Revision History

- Version 1.0 – Initial publication (2025)

Disclaimer

This technical guidance outlines recommended best practices. Organizations remain responsible for implementing measures appropriate to their specific risk environment and ensuring compliance with the Somalia Data Protection Act No. 005 (2023).