هيئة المعلومات والحكومة الإلكترونية
Information & eGovernment Authority

Governance & Enterprise Architecture Directorate

Backup Policy

Version 1.1 | 08 August 2024

Document Control

Attributes	Value
Document Title	Backup Policy
Document Owner:	Governance & Enterprise Architecture Directorate Information and eGovernment Authority
Publication Date:	08 August 2024
Number of Pages:	11 Pages
Caution:	This document is controlled electronically. Printed copies are treated as uncontrolled and cannot be guaranteed to be the current version

Document Review

Version	Author	Status	Date	Remarks
1.1	Governance & Enterprise Architecture Directorate	Published	08 August 2024	• Minor changes in phrasing and content organization. • Added Document Control and Document Review sections. • Clarified types for each backup frequency.
1.0	Governance & Enterprise Architecture Directorate	Published	06 April 2023	First version released.

Table of Contents

Glossary

Acronyms	Definition
CSB	Civil Service Bureau
ICTGC	Information and Communication Technology Governance Committee
iGA	Information and eGovernment Authority
MCICT	Ministerial Committee for Information and Communication Technology
MOFNE	Ministry of Finance and National Economy
NCSC	National Cybersecurity Center
SaaS	Software as a service

1. Introduction

This backup policy aims to ensure the regular, secure, and reliable backup of critical business data across all government entities. It outlines the procedures for data backup, restoration and recovery from data loss, disasters, or system failures. The policy addresses the risks associated with data loss and underscores the benefits of a robust backup strategy.

2. Objective

To achieve comprehensive data protection by:

- Safeguarding critical data through regular backups.
- Ensuring swift restoration of operations after data loss incidents.
- Maintaining compliance with relevant data protection laws and standards.

3. Scope

This policy must be applied to all files and databases that are essential and mission-critical for government entity's business operations, applications, and systems, whether they are hosted on-premises or on cloud.

4. Policy

4.1 Planning and Requirements

4.1.1 Government entities are responsible for identifying the business applications and its associated data and files.

4.1.2 A formal Backup Plan shall be documented by government entities in cooperation with the Information and eGovernment Authority. The plan must be reviewed and signed by both parties.

4.1.3 The Backup Plan shall be reviewed and updated on a regular basis (at least yearly) or on demand upon changes in business requirements.

4.1.4 The review of backup plan should consider the inclusion of new systems or exclusion of obsolete systems.

4.1.5 The Backup Plan must document the following details for each system or application:

- List of business applications and systems with their owners that needs to be backed-up.
- Backup frequency and retention.
- Details on all backup locations.
- The name of Entity's Backup Coordinator(s) responsible for all relevant activities including backup, testing, validation, restoration, destruction.
- The name of coordinated iGA Department.
- iGA and government entity's signature, and the date of the approval.

4.2 Backup

4.2.1 Government entities are responsible for activating the backup as per the backup plan.

4.2.2 As a minimum requirement, the backup must be taken based on the following manner:

Backup Frequency	Retention Period	Type
Daily	35 Days	Incremental
Monthly	13 Months	Full
Yearly	5 Financial Years	Full

4.2.3 A 3-2-1 Backup rule must be implemented as follows:

- There must be three instances of the data:
- Primary Data: The original data residing in your on-premises or cloud environment.
- Local Backup: A first backup copy stored within the same on-premises or cloud environment but in a separate location.

- Offsite Backup: A second backup copy stored in a geographically distinct location outside the primary on-premises or cloud environment. This copy must be protected from direct access from the main environment. The Information and eGovernment Authority can assist other government entities in managing and maintaining this backup copy upon request.

4.2.4 Special or additional requirements for backup frequency or retention periods shall be identified by the respective government entities and formally communicated to Information and eGovernment Authority.

4.2.5 Information and eGovernment Authority will be responsible for standardizing suitable backup solution for government entities.

4.2.6 Government entities will be responsible for the whole cost of their backup needs, including hardware and software licenses.

4.2.7 Backup must be protected with appropriate security controls defined by the National Cybersecurity Center (NCSC) with consideration to data-related laws listed in the References section of this document.

4.2.8 Onsite and offsite backup media must be available to, and accessible by, Entity's Backup Coordinator and an authorized iGA IT Administrator(s) as defined in the Backup Plan.

4.2.9 Time-stamped backups logs must be maintained for all critical and important systems including the following details:

- Date and time of backup.
- Whether back up completed successfully.
- Reasons for unsuccessful back up (if any).
- Details on offsite and onsite storage media.
- Details of the Entity's Backup Coordinator(s) responsible for the backup.
- Details of coordinated iGA Department.

4.2.10 Failures in the backup procedure must be reported to the concerned department(s) in both the entity, and the Information and eGovernment Authority.

4.3 Testing and Validation

4.3.1 Government Entities, in coordination with Information and eGovernment Authority, must conduct testing and validation for all critical mission system once in every six months.

4.3.2 testing and validation shall verify successful restoration of the backup copies with consideration to compatibility with existing systems.

4.3.3 A proper schedule for backup testing and validation must be documented for all backups and communicated to Information and eGovernment Authority.

4.3.4 Time-stamped testing and validation logs must be maintained that include the following details:

- Date and time of backup and restore validation.
- Whether both backup and restoration completed successfully.
- Reasons for unsuccessful backup or restoration (if any).
- Details of Entity's Backup Coordinator(s) responsible for the validation.
- Details of coordinated iGA Department.

4.3.5 Failures in the validation procedure must be reported to the concerned department(s) in both the entity, and Information and eGovernment Authority.

4.4 Restoration

4.4.1 Restoration procedures should be initiated by Entity's Backup Coordinator in coordination with Information and eGovernment Authority.

4.4.2 Restoration procedure will be only initiated in the event of disaster, system failures, corruption of information, loss of data or based on special business requirement.

4.4.3 A time-stamped restoration log must be maintained to include the following details:

- Date and time of restoration.
- Reason for restoration.
- Whether restoration completed successfully.

- Reasons for unsuccessful restoration (if any).
- Details of Entity's Backup Coordinator(s) responsible for the restoration.
- Details of coordinated iGA Department.

4.4.4 Failures in the restoration procedure must be reported to the concerned department(s) in both the entity, and Information and eGovernment Authority.

4.5 Backup for Cloud-based Productivity Applications

4.5.1 This policy may apply to users' data hosted on premises and cloud (such as emails and documents).

4.5.2 Backup Frequency: Incremental backup for 90 days.

4.5.3 Retention Period: up to 5 years.

5. Exemptions

- All exemptions to this policy shall be explicitly identified by the respective government entities and formally communicated to Information and eGovernment Authority.
- Information and eGovernment Authority will review exemption request and has the right to approve or reject it based on respective government laws, regulations, policies, standards, and business needs.
- Information and eGovernment Authority has the right to present the exemption request, if necessary, to Information and Communication Technology Governance Committee (ICTGC).

6. Responsibilities

The following table summarizes all responsibilities mentioned in this policy:

	Entity	Responsibilities
1	**Government Entities**	- Identify and prioritize the business applications, system and its associated files and databases. - Assign a Backup Coordinator to arrange all backup-related matters. - Define and approve the Backup Plan in coordination with Information and eGovernment Authority. - Manage, activate, maintain, and execute all relevant activities including backup, restoration, and validation in coordination with Information and eGovernment Authority. - Cover the cost of backup requirements, including hardware and software licenses.
2	**Information and eGovernment Authority (iGA)**	- Reviews the Backup Plan in coordination with respective government entities. - Assigns a department responsible for coordinating backup activities with the entities. - Standardizes suitable centralized backup solution for government entities. - Oversees policy implementation to ensure consistency and effectiveness, and reports to ICTGC / MCICT accordingly.
3	**Information and Communication Technology Governance Committee (ICTGC)**	- ICTGC is the approval authority for major change in the policy. - ICTGC takes decisions on special or additional requirements, including exemption requests raised by government entities.
4	**Ministerial Committee for Information and Communication Technology (MCICT)**	- MCICT sets the strategic directions for the policy

7. Enforcement

This policy is established based on Ministerial Committee for Information and Communication Technology (MCICT)'s decision number 05/2023-08. The policy must be applied to all files and databases that are essential for government entity's business operations, applications, and systems, whether they are hosted on-premises or on cloud.

8. References

Data-Related Laws

1. Government Data Protection Law No.16 (2014).
2. Personal Data Protection Law No.30 (2018).