هيئة المعلومات والحكومة الإلكترونية
Information & eGovernment Authority

Governance & Enterprise Architecture Directorate

Backup Policy

Version 1.0 | April 2023

Table of Contents

1. Objective

To ensure that backup copies of critical business data, are taken regularly in a secure and reliable manner such that it is available for restoration of business operations when needed in the event of data loss, disasters, or system failures.

2. Scope

This policy must be applied by all government entities on the mission critical systems, including those hosted on premise and on cloud environments.

3. Policy

3.1 Planning and Requirements

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

3.1.2 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.

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

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

3.1.5 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.

3.2 Backup

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

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

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

3.2.3 A 3-2-1 backup strategy must be implemented based on the following:

- There must be three copies of the data.
- Two copies must be stored separate from each other.
- One copy must be stored on an offsite storage (different geographical location), and it must be offline (disconnected from network or any devices). This copy is mandatory for all mission critical systems, and it can be managed and maintained by Information and eGovernment Authority.

3.2.4 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.

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

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

3.2.7 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.

3.2.8 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.

3.2.9 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.

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

3.4 Testing and Validation

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

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

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

3.4.3 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.

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

3.5 Restoration

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

3.5.2 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.

3.5.3 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.

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

3.6 Backup for Cloud-based Productivity Applications

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

3.6.2 Backup Frequency: Incremental backup for 90 days.

3.6.3 Retention Period: up to 5 years.

4. 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 the national ICT Governance Committee (ICTGC).

5. Responsibilities

The following table summarizes all responsibilities mentioned in this policy:

	Entity	Responsibilities
1	Government Entities	- Identify the business applications, system and its associated data, files. - 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.

	Entity	Responsibilities
4	Ministerial Committee for Information and Communication Technology (MCICT)	- MCICT sets the strategic directions for the policy

6. Enforcement

This policy is established based on Ministerial Committee for Information and Communication Technology (MCICT)'s decision number 05/2023-08. The policy is to be implemented on all mission critical systems, including those hosted on the cloud services.

7. References

Data-Related Laws

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