This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise must be edited appropriately. Items highlighted in green are examples and must be removed. After all edits have been made, all highlights must be cleared.

Insert organization logo by clicking on the outlined image.



# Backup Policy Template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Choose Classification

| | |
|---|---|
| DATE: | Click here to add date |
| VERSION: | Click here to add text |
| REF: | Click here to add text |

# Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

# Document Approval

| Role | Job Title | Name | Date | Signature |
|---|---|---|---|---|
| Choose Role | <Insert job title> | <Insert individual's full personnel name> | Click here to add date | <Insert signature> |
| | | | | |

# Version Control

| Version | Date | Updated By | Version Details |
|---|---|---|---|
| <Insert version number> | Click here to add date | <Insert individual's full personnel name> | <Insert description of the version> |
| | | | |

# Review Table

| Periodical Review Rate | Last Review Date | Upcoming Review Date |
|---|---|---|
| <Once a year> | Click here to add date | Click here to add date |
| | | |

# Table of Contents

# Purpose

This policy aims to define the cybersecurity requirements related to the backup and recovery of all of <organization name>'s information and technology assets to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

# Scope

This policy covers all <organization name>'s information and technology assets (e.g., systems, data and information) and applies to all personnel (employees and contractors) in the <organization name>.

# Policy Statements

1- **General Statements**

1-1 All IT systems (including cloud, remote access, telework, and critical systems) in <organization name> must have defined processes and procedures.

1-2 System owners are accountable for the creation of the defined backup processes and procedures, assisted by business representatives.

1-3 When <organization name>'s information technology assets (systems, data and information) are to be backed-up, the business owner and representatives of <legal function> and <data protection function> must assist in the creation of the required backup processes and procedures.

1-4 Physical and logical access to <organization name>'s backups, backup media (physical and online) and restoration capabilities must be restricted and limited to authorized users only. Additionally, any physical and logical access privileges to these mediums must be reviewed periodically, at least once a year.

1-5 The access, storage and transfer of all systems' backups, cloud services tenants' data backups and the media used for these backups must be protected against damage, amendment or unauthorized access.

1-6 Cybersecurity requirements for backup, retention and restore must meet legal and regulatory requirements, be reviewed at least once a year, and reviewed when there are changes in the relevant legal and regulatory requirements.

1-7 Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements for backup, retention and restoration.

## 2- Backups

2-1 Backup media must be tested periodically and at least once a year to ensure it meets the manufacturer's stated specifications, is free from physical fault(s), functions as intended and replaced where required.

2-2 Backups must be taken at regular intervals, to meet legal and regulatory requirements and as defined by the <organization name>.

2-3 A business impact assessment must be conducted to determine the frequency and type of backup required for each system.

2-4 Daily backups must be performed for all the components of critical systems.

2-5 Online backup (which makes use of a remote or cloud-based storage system to get the data to be stored in a server that is connected to the network) and offline backup (which makes use of a physical piece of hardware such as an external hard disk, DVD, memory card, etc. that is isolated from any network or online device to store the data) must cover all critical systems' components.

2-6 Offline and physical backup media must be stored off-site in an approved secure location, preferably at a physically remote location.

2-7 Online backups must be stored separately from production, test, development, office and operational technology environments and networks.

3- **Retention**

3-1 <organization name> backups must be retained for defined time periods as required by legislation, regulation, business policy (e.g., <Information Classification Standard> and <Data Retention Standard>) and business needs.

3-2 Backups must be reviewed at specified time periods to ensure they meet all retention requirements, such as legislation, regulation and business need.

4- **Backup deletion**

4-1 Backups must be deleted only after obtaining owner's approval.

4-2 Physical backup media must be deleted and destroyed securely, when required.

4-3 Online backup media must be deleted and erased securely, when required.

5- **Restore**

5-1 Restoration testing must be conducted at least once a year for all backups.

5-2 Restoration testing must be conducted once every three months for critical systems' backups.

5-3 Restoration testing must be conducted once every six months for remote work systems' backups.

5-4 <organization name> must be able to restore its backup within a defined time frame in alignment with its business needs, targeted Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

## Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

## Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

## Compliance

1- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.