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

Insert organization logo by clicking on the outlined image.

Backup Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

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”

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 standard aims to define the detailed cybersecurity requirements related to the backup and recovery of all of <organization name>'s information technology assets to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability

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

Scope

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

Standards

1	Data backup and recovery processes
Objective	To define a backup process for each IT system used by <organization name>
Risk implication	Lack of a backup process may result in the loss of data and information in the event of a system error, unplanned shutdown or compromise. Lack of a backup process may mean that an IT system cannot be restored to a known time point and known condition, adversely affecting business operations and placing <organization name> in breach of legal or regulatory obligations.
Requirements	
1-1	Data backup processes and procedures must be defined for all IT systems, including cloud, remote access, telework and

	critical systems, used by <organization name> including third party hosted systems in alignment with <organization name>'s Data Classification Standard.
1-2	A Business Impact Assessment (BIA) must be carried out by the system owner and business users of the system to determine the frequency and type of backup required.
1-3	Recovery Time and Recovery Point Objectives (RTO and RPO) must be determined by the system owner and business users of the system using the results of the Business Impact Assessment (BIA).
1-4	System owners must be responsible for defining the data backup processes and procedures for the systems for which they have responsibility. At a minimum, data backup processes and procedures must include the following requirements: a) authorized personnel with access to backups and backup media b) operational procedures c) backup logging procedure d) frequency (e.g. daily, weekly or monthly) to meet business impact analysis Recovery Time and Recovery Point Objectives e) a record of system and application files to be backed up (e.g. operating system, or application executables) f) a record of data and information to be backed up (e.g. static data, customer files or transaction records) g) backup type (e.g. incremental or full) h) medium (e.g. tape, disk, cloud) i) storage (e.g. onsite, offsite, rotation) j) records of backup (e.g. date, media and storage location) k) retention periods

	l) log monitoring and error resolution procedures (e.g. rerunning a failed backup within a set timeframe) m) testing procedures (e.g. backup verification) n) data restoration procedures and timescales o) data encryption requirements
1-5	The use of personal removable media of any kind (e.g., external USB drives) as a backup medium must be prohibited.
2	Protection of backup media
Objective	To protect backup media
Risk implication	Unprotected or improperly stored and handled backup media can be damaged, lost, stolen or compromised. Damage to backup media may adversely impact the restore of an IT system or associated data and information; loss or theft may mean that a restore cannot be carried out and, depending on the data and information stored on the backup media, may expose <organization name> to legal or regulatory investigations and penalties.
Requirements	
2-1	Backup media must be stored in a secure and fireproof location when not in use and protected from environmental risks (e.g., flooding).
2-2	Backup media must be stored separately from live media (i.e., streaming media) using online storage (such as implementing a dedicated backup network or implementing network physical and/or logical segmentation).
2-3	Access to backup media must be restricted and limited to authorized personnel with appropriate business need.
2-4	Authorized personnel who can access backup media and the justification of access must be identified and documented.

2-5	Physical backup media (e.g. disks, tapes, etc.) must be moved to a <organization name>'s approved secure offsite location immediately after creation or use.
2-6	Physical backup media must be transported to and from offsite locations using a secure method of transportation (such as a dedicated courier and security box).
2-7	The ability to recall offsite backup media must be restricted to authorized personnel.
2-8	All requests for the recovery of backup data must be logged in a centralized location (i.e., a backup request log). The backup request log must record, at a minimum: a) the time of the request b) the identity of the individual making the request c) the business reason for the request d) the system backup required e) identity of individual approving or denying the request (denials must be accompanied with a reason why the request was denied).
2-9	The backup request log must be stored in a secure manner, with access limited to authorized personnel, using physical and logical access controls.
2-10	Review and inventory at least annually all physical backup media.
2-11	Physical backup media must be replaced before they reach manufacturer's stated end of life.
3	Backup test and restore
Objective	To test data backup data for completeness and restoration
Risk implication	Damage to or corruption of backup media and corruption of data and information stored on the backup media will not be

	identified. This may adversely impact the restore of an IT system or of the associated data and information
Requirements	
3-1	All backups must be tested and verified after they have been run to ensure the backup taken has been done successfully. For example, checking file size, using hash totaling or deploying other methods of verification.
3-2	A backup restoration test must be conducted periodically as the per the following: - once a year for all backups. - once every three months for critical systems' backups. - once every six months for remote work systems' backups.
3-3	The restoration test must be reviewed to check if the restoration occurred within or met defined timescales.
4	Protection of online backups
Objective	To protect online backups
Risk implication	Improper, or no, protection of online backups may result in unauthorized access, modification or deletion of backup data and information. This may adversely impact the restore of an IT system or associated data and information.
Requirements	
4-1	Physical and logical access to online backups (e.g. Network Attached Storage, Storage Area Networks or cloud) must be restricted and limited to authorized personnel only.
4-2	Backup storage, either online or offline, must be encrypted either by encrypting individual backup files and/or the storage volume.

4-3	Backup files must be encrypted when transferred or transmitted across the networks and physical locations.
5	Backup and data retention requirements
Objective	To retain and manage data and backups according to legislation, regulation and policy
Risk implication	Retaining data and information for incorrect periods of time may lead to breaches of legislation, regulation and policy.
Requirements	
5-1	Data and backups must be retained for defined time periods as required by legislation, regulation, and business policy in alignment with <organization name>'s Asset Classification Standard and Data Protection Policy.
5-2	Data and backups must be reviewed at least once a year to determine if defined retention periods have been exceeded, and the results of the review must be documented.
5-3	Data and backups containing personal information must be reviewed at least once every six months to determine if defined retention periods have been exceeded, and the results of the review must be documented.
5-4	The system owner must define a process to delete data and backups upon request in alignment with <organization name>'s Data Protection Policy. The process must include the following minimum requirements: a) how a request for data/backup deletion is to be submitted (for example in an email) b) the recipients of a deletion request (e.g., system owner, <legal function> representative, data protection officer) c) who can request data/backup deletion (e.g. <organization name> personnel)

	d) who can authorize the issue of data/backup deletion (e.g. <legal function>) e) who can delete data/backups, or create an automatic delete activity (e.g. <Information technology function>) f) how long a request to delete data/backup will take g) what mechanism will be used to prove deletion has occurred and is permanent h) how encryption keys (if used) will be destroyed i) how the request and deletion is recorded in a secure manner.
5-5	All requests for the deletion of backup data must be logged in a centralized location (the backup deletion log). The backup deletion log must record, at a minimum: a) the time of the request for deletion b) the identity of the individual making the request for deletion c) the business reason for the deletion d) the system backup to be deleted e) date and time for the actual deletion f) the name of person/personnel who deleted it g) identity of individual approving or denying the request (denials must be accompanied with a reason why the request was denied).
5-6	The backup deletion log must be stored in a secure manner, with access limited to authorized personnel, using physical and logical access controls.
5-7	Destruction of physical backup media must be in alignment with <organization name>'s Asset Classification Standard and Physical Security Standard.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

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

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

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

Update and Review

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

Compliance

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

2- All personnel at <organization name> must comply with this standard.

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