TANZANIA MENTORS ACTION

DATA STORAGE, BACKUP AND RECOVERY POLICY

Revised Version 2023

Table of Contents

1. **Our Vision**

   To have a society that is healthy and capable of contributing fully to the development of individuals, communities, and the nation at large.

2. **Our mission**

   To empower leaders, service providers and citizens across all levels of governance to deliver demand driven quality services by promoting both downward and upward accountability through various methods including mentorship.

3. **TMA Core values**

Excellence	We are committed to providing services that are distinctive and of high quality.
Innovation	We are innovative in our designs and operations, using technology and modern ways of doing business to further satisfy the needs and expectations of the customer.
Integrity	We value responsible character with impeccable levels of integrity for all individual members, office bearers and staff of TMA, in and outside TMA programming.
Commitment	We are fully committed to all our pledges and engagements.
Respect	We accord due regard to the feelings, wishes, and rights of others.
Transparency	We are transparent to our members, staff and stakeholders in all we do.
Accountability	We are guided by the highest possible standards of internal and external accountability to all our stakeholders, and we comply with all statutory requirements.
Equality	We believe that all human beings are equal in dignity and before the law.

Gender Sensitive	We are sensitive to gender needs and understand that equality is not the same as equity.
Diversity	We cherish and respect diversity in terms of culture, religion, political opinion, social origin and style of doing things provided the said diversity does not infringe the law.

4. Definitions

For purposes of this policy and associated rules, the following words and phrases shall be defined as follows:

1. **Backup** - saving of files onto magnetic tape, disk, other mass storage media or in the cloud for the purpose of preventing unplanned data loss in the event of equipment failure or destruction.
2. Application Owner – The user, department, or team that maintains or manages the application or data that is being backed up.
3. **Data Retention** - The saving of historic and/or inactive files on disk, or other mass storage media for the purpose of keeping it for compliance or legal reasons, for a defined period.
4. **Backup Retention** – The time lapse between when a backup is created and when it is formatted to be destroyed or potentially reused. This can be considered the ‘shelf-life’ for the backup and is how long the backup will be kept before the images are expired. Backups will be saved onto magnetic tape, disk, or in the cloud.
5. **Data Recovery** – The purpose of backing up data is to store a copy of the data in the event of a disaster where data is lost or corrupt. Data recovery is the act of restoring data from the backup to restore data to the desired point in time.
6. **Recovery Point Objective (RPO)** – is the maximum targeted period in which data might be lost from an IT service. The RPO is the age of files that must be recovered from backup storage for normal operations to resume. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs (e.g., a high transactional DB data is only good for 5 days. The RPO is 5 days ago or sooner).
7. **Backup Software** – The software used to manage the data backups and recovery (e.g., Commvault, NetBackup Enterprise Server).

5. Policy Statement

It is the policy of TMA to maintain back-up copies of electronic data files off-site in a secure, fire-protected environment. Access to back-up files shall be limited to individuals authorized by management.

6. Purpose and Scope

1. The purpose of this policy is to document the TMA data backup and recovery procedures, protocols, and standards. This policy covers the data backup schedule, backup protocols, backup retention, and data recovery.
2. This policy assumes Application Owners will notify the ICT Unit, with the applications designated: recovery point objective (RPO), timing for when the backups should take place, and compliance requirements as they pertain to data backup and recovery.
3. The ICT Unit will only be responsible to manage the infrastructure, backup, and recovery of application data.

7. Objectives

a. To ensure organizational data is stored in an on and off-site location and can be easily found and recovered in the event of an equipment failure, intentional destruction of data, or disaster.

b. To covers the infrastructure and procedures that are provided for organizational data backup and recovery.

8. Rules, Procedures, and Guidelines

The following information outlines the policies with respect to data backup and restore.

a) The ICT Unit will be responsible for all aspects of backing up servers provided by TMA. Test servers and Trial Operating Systems will not be backed up, unless requested by the owner.

b) Backups will include daily incremental, weekly, and full monthly backups as defined by service or application owner. This team will also be responsible for finding and restoring data when requested or required for Disaster Recovery purposes.

c) Procedures regarding Target Media (e.g., Tape, Disk, and Cloud)

i. ICT Unit is responsible for maintenance and support

ii. The following are backup schedule and Backup retention frequency:

a) Daily backups
    i. Incremental and full backups will be kept on-site for 1 month
    ii. Full backups will be stored on- and off-site for 3 months
    iii. Tapes may be reused as they expire if they are still viable

b) Weekly Production Backups
    i. Full and incremental weekly backups will be stored on-site for 1 month
    ii. Full backups will be stored on- and off-site for 3 months
    iii. Occur as scheduled; 4 iterations per month
    iv. Tapes may be reused as they expire if they are still viable
    v. Duplicate copy of weekly backup will be stored securely off-site and retained for 3 months

c) Monthly Production Backups
    i. Full and incremental backups will be stored on-site for 3 months ii. Full backups will be stored on- and off-site for 6 months
    ii. Monthly Vault Full backups to tape will be stored off-site for 3 months and on-site for the remainder of the year
    iii. Tapes may be reused as they expire if they are still viable

d) Non-production
    i. Non-production environments will be retained for 1 week
    ii. Will not be sent off-site

e) Special Backup Requests (i.e., litigation, system upgrades, retirements etc.)
    i. Full backups may be sent off-site upon request
    ii. Copies may be set up for up to 6 months' retention iii. Backup retention can be used as data retention
    iii. Backup retention special requests will require a written Service Level Agreement (SLA), presented to the TMA Security Officer, Head of ICT Unit, and/or governance groups

9. Store, Backup and restores Policy configuration:

i. It is the responsibility of the ICT Unit to make sure backups are running as scheduled

ii. The ICT Unit will verify that backup jobs have completed successfully and will contact workers if problems occur.

iii. Workers will be given problem ticket number with ICT Unit when server problems occur and for making a follow-up.

iv. When a new server is added to the production environment, the administrator of the server will contact the ICT Unit to have the server added to the backup system

10. Regarding Data Restores

a. Restore requests will be submitted to the ICT Unit

b. Restores that require a tape from off-site storage will be started within 72 hours

c. All other restores will be started within 2 hours business hours

d. Restores over weekends/holidays will be performed the following business day, unless an urgent/high ticket is submitted

10.1 The ICT Unit will be responsible for the following:

i. Ordering backup media, cleaning tapes, and labels

ii. Checking backup reports to ensure that they were completed without errors

iii. Report any problems with the backup software to the workers that includes Troubleshooting steps taken and Any errors found

iv. Making sure the library has tape media available for backups and offsite storage

v. Packing monthly backup and sending them to the vault

vi. Updating clients/servers to current version after upgrades when feasible with assistance from the customer if necessary.

vii. Install updates/upgrades of the backup software.

viii. Managing relationships with storage vendors.

ix. Maintaining storage arrays

x. Executing this policy

xi. Contact vendor when necessary for troubleshooting.

10.2 The ICT Unit will NOT be responsible for the following:

i. Troubleshooting and investigating what caused data loss or data corruption on client computers

ii. Lost production data because of end-user changes to an application or application data

iii. Lost data that falls outside of the backup

10.3 Disaster Recovery Alternate Site

The policy for the disaster recovery alternative site will be the same as the production data center with the following exceptions:

a) Internal applications

b) External application

10.4 Exceptions

There shall be no backups performed of the data stored on user devices, such as desktops, workstations, and/or laptops. Any exceptions to the data backup policy will require the explicit written approval of the ICT Head of Unit.

10.5 Restoration

Users who need files restored must submit a request to ICT Unit, and they will need to include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

10.6 Encryption

Backups shall be performed with at least 128-bit. Encryption keys are replicated from the Downtown Data Center to alternate site.