Backup and Restore Policy CGICT_ICT_003

Version 1.3 June 2021

Version Control and Approval			
Document Name		Backup and Restore Policy	
Document Number/Version		1.3	
Status/Revision History			
Rev #	**Revision Update**	Revised By	Date
1.0	**New**	Author: William Nkuna	April 2017
1.1	Revision	Author: William Nkuna	September 2019
1.2	Revision	Author: Ray Mtetwa	November 2019
1.3	Revision	Author: Mpumelelo Khumalo, Ebrahim Mayet	June 2021
Approval			
Date Approved			
Date Last Amended		June 2021	
Date of Next Review		2023/24	
Related Policies		Information Security Policy, ICT Governance Framework	
Authored By			
Name		Mr. Mpumelelo Khumalo	
Position		Acting ICT Manager	
Signature			Date: 30/03/2022
Reviewed and Recommended by			
Name		Ms. Sibongile Ngwenya	
Position		Executive Manager: Corporate Services	
Signature			Date: 30/03/2022
Name		Mr. Thamsanqa Mdontswa	
Position		Chief Executive Officer	
Signature			Date: 30/03/2022
Approved By			
Name		Ms. Portia Mushwana	
Position		Chairperson : ICT Steering Committee	
Signature			Date: 30/03/2022

Backup and Restore Policy
CGICT_ICT_003

Version 1.2 November 2019

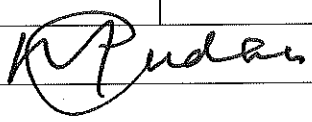
Approved By		
Name	Mr. Chris Mudau	
Position	Chairperson: Board and Accounting Authority	
Signature		Date: 14/04/2022

Table of Contents

1 Introduction

Information Communication and Technology systems and electronic data are valuable assets to SASSETA (Safety and Security Sector Education and Training Authority) and a substantial investment in human and financial resources has been made to create these systems and information and, as such, a formalised policy has been implemented to:

- Safeguard the risk of losing data
- Safeguard the confidentiality and integrity of information contained within these systems
- Ensure availability of critical data so that information can be utilized as a valuable asset
- Reduce business and legal risk
- Ensure business continuity

Departmental critical data and non-departmental critical data are stored on Fileservers, Exchange-servers (mailbox data),Application-servers and Cloud Services (Microsoft OneDrive). This data can be categorised as:

- Official Business data stored on personal computers and devices
- Business Unit data stored on Shared Drive
- Databases
- Application / System data
- Operating and Application software

The Safety and Security Sector Education and Training Authority (SASSETA) developed this backup policy for systems within the organisation, which are expected to have their data backed up. These systems are typically servers, but are not necessarily limited to servers. Servers are expected to be backed up including the file or data server, the mail server, application servers and cloud services. Where information or data is stored on a desktop computer and that information is critical for the survival of SASSETA, a mechanism has been provided to backup that data on the cloud via OneDrive.

2 Purpose

This policy is designed to protect data against loss and to ensure recovery in the event of equipment failure, intentional destruction of data, business disruption or a disaster situation. The purpose of the Data Backup and Restore Policy is to provide for continuity, restoration and recovery of critical data and systems.

3 Scope

This policy has been designed with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as a key deliverable and is therefore not designed as a method of archiving material for extended periods.

The 'data' backups cover all systems managed by the ICT department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with ICT Staff.

This policy applies to data owned and operated by SASSETA. It is applicable to data stored on all equipment belonging to SASSETA. It further includes data stored at the premises of the service providers or third parties used for the SASSETA purpose.

4 Definitions and Terms

Term/Acronym	Definition
Backup	The activity of creating a copy of a file(s) and/or folders which are stored separately from the original data, to preserve in the event of accidental data loss, disasters or due to data that is inaccessible. It is also the process of copying active files from online disk to cloud so that files may be restored to a disk or server in the event of equipment failure, damage to or loss of data.
Archive	The process of moving inactive files from online disk to a specific location, i.e. deleting the files from copying them, in order to release online storage for reuse. It is also the process of moving inactive files from online disk to the cloud, i.e. deleting the files from copying them, in order to release online storage for reuse.
Restore	Process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

5 Guidelines and business rules

a) Timing

Incremental backups will be performed daily from Monday to Friday. The backups will be on the cloud as well as the internal backup server and will be updated with new information as it is created.

A full system and data backup will be performed every Saturday.

Monthly backups will be made on the last Friday of each month and stored on the cloud for a minimum period of 5 (five) years or as required by legislation.

b) Cloud Storage

All backups within SASSETA will be stored on the cloud (external online servers managed by a third party). These backups will be maintained as follows:

i. Daily and Weekly backups

Each Friday of the month such as Friday1, Friday2, etc. backups performed on the Friday or weekends shall be kept for one month and thereafter deleted and archived to free the space for the next months backup. Backups performed Monday through Thursday shall be kept for one week and thereafter deleted and archived to free space for the next weeks backup.

ii. Monthly Backup

On the last day of each month, a monthly backup shall be performed and stored on the cloud. The monthly backups will be kept for a period of five (5) years. On the sixth year, the first year's monthly backup will be deleted and archived to free the cloud storage for that year's backup. Where there is a legislative requirement to keep the backup for more than five (5) years, the backups will be archived for a stipulated period in accordance with the legislation.

6 Roles and Responsibilities

The ICT manager shall delegate a member of the ICT department to perform regular backups. The delegated person shall develop a procedure for performing backups and test the ability to restore data from backups on a quarterly basis.

All staff are reminded that they are individually responsible for data held locally on their desktop computers or laptop computers and all business data *must* be stored on the network drives provided or central online services.

Where a system(s) and or data is managed by a external service provider, a clause in the service level agreement shall be included and enforced with the service provider to perform and test the backups of the system or data belonging to SASSETA in line with this policy. The test results will be shared with SASSETA on a quarterly basis in line with this policy.

RACI Matrix

Backup Component	Responsible	Accountable	Contribute	Inform
Data Criticality "Rating"	ICT Application Team	ICT Application Team	ICT Team	ICT Backup Operator
Detailed Application/Server Build Documentation	ICT Application Team	ICT Team	ICT Backup Operator	ICT Backup Operator
Data Backup Selection List	ICT Team	ICT Application Team	ICT Backup Operator	ICT Backup Operator
Backup Monitoring (Including failed backups)	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Backup Reporting	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Media management	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Offsite Storage	Offsite Data Custodians	ICT Backup Operator	ICT Team	ICT Application Team

7 Testing of backup

The ability to restore data from backups must be tested at least once a quarter or three months period.

i. Testing of the restore of hosted applications

A restore of the data of hosted applications must be done on a quarterly basis. The restore will be as per the requirement of the end user or possible sample suggested by the ICT Department. The results of the restore should be documented and kept as proof of the restore.

8 Backup Selection

8.1. All data and software essential to the continued operation of SASSETA, as well as all data that must be maintained for legislative purposes, must be backed up.
8.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
8.3 The application owner, together with the ICT, will determine what information must be backed up, in what form, and how often.

8.4 Data to be backed up include the following information:

1. User data stored on the hard drive
2. System state data (boot files, SysVol -DCs)
3. Registry Files (Servers)
4. Network Drives Files stored on the Fileserver
5. Financial Systems data (including Supply Chain Management)
6. HR Systems data
7. Other Applications System data
8. Intranet and Extranet website Files
9. Hyper V Infrastructure
10. Emails (Office 365)

Web based systems will be backed up by the respective service providers.

8.5 Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Operating Systems software
7. Test database server
8. Test web server
9. Application Servers

10. Third party managed systems – A clause in the SLA regarding the backups shall be included to ensure that SASSETA data is not lost.

9 Archives

Archives are made at the end of every financial year in April. User account data associated with the file and mail servers are archived one month after the users have left the organisation.

10 Restore Process

The following steps specify the backup restore process:

a) The backup restore will only be performed in case of disaster or as part of quarterly routine testing.
b) The backup restore will be performed on official request to ICT.
c) Information regarding the request for restore should include file name, file creation date, the last time it was changed and the date and time it was deleted or destroyed.

11 Off-Site Storage Location

Backups for SASSETA managed systems must be stored on the cloud backup managed by an external service provider. An SLA with the service provider must be completed and signed by both parties stipulating the procedures for backup and restore; and adherence to the laws and legislation governing the security and confidentiality of the data.

12 Policy Implementation

The ICT Business Unit and Corporate Services is accountable and shall also be responsible for its future amendments or reviews.

The CEO is accountable for the overall policy implementation and reserves the right to intervene and take necessary steps when the policy is not adhered to. The accountability may be delegated to the Corporate Services Executive or any other manager deemed fit for the function. Business Unit Heads, in consultation with ICT, are responsible for policy implementation in their respective divisions.

13 Non-Compliance to the Policy

The policy should be used in conjunction with the SASSETA Disciplinary Policy, where disciplinary action could be a consequence due to non-compliance.

14 Policy Validity

This policy will be effective from the date of approval, however the current policy will still be in place and will complied with. In an event of any doubt about the authenticity of a policy document, the document signed by the CEO shall be considered as the only document with validity, authority and a force of law.

ANNEXURE A

The below strategy is used as a guideline, alternatively the ICT Manager can revise the strategy that must be strictly adhered to:

Data Set	**Full Backup**			**Incremental Backup**
	Monthly	**Weekly**	**Yearly**	**Daily**
Financial Systems	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday
HR Systems	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday
File Services	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday
Mail	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday
Indicium	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday
Data Proof	Last Friday of the month	Every Friday	Weekend after Financial Year end	Monday to Thursday