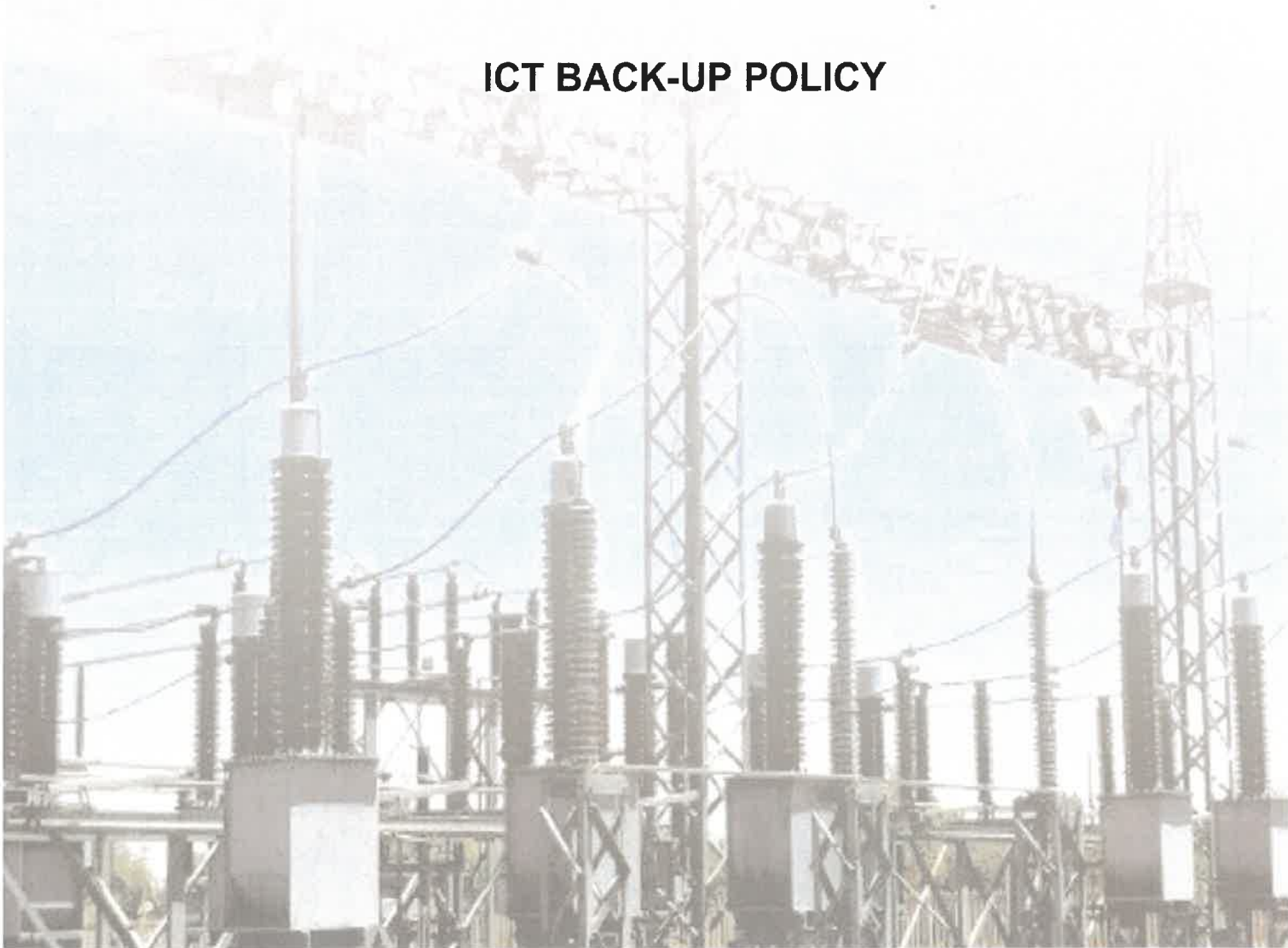




ICT BACK-UP POLICY





DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: ICT BACKUP POLICY	POLICY NO:
REV NO: 1	REV DATE: 10 May 2023
SUB-DIRECTORATE: Information Management	BOARD ITEM NO:
SIGNATURE:	
DATE APPROVED:	EFFECTIVE DATE: 01 July 2023

Definitions:

Archive: the saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Backup: the saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Degaussing: is a process of decreasing or eliminating a remnant magnetic field on a floppy disc or tape.

Dry run: is a testing process where the effects of a possible failure are intentionally mitigated.

Restore: the process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

1. OBJECTIVES

- To protect the entity's data such that there is assurance that it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

2. POLICY PRINCIPLES

- a) This policy is directed by the principle of proper backup, storage, and handling of data in order for the entity to achieve its objectives efficiently in an effort to preserve information relating to its operations.
- b) Staff must protect the availability, confidentiality and integrity of entity's data.
- c) Furthermore, data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure.
- d) Backup provisions should be understood and executed from the perspective that will allow business processes to be resumed in a reasonable amount of time with minimal loss of data.
- e) Since hardware and software failures can take many forms, and may occur over time, multiple generations of entity's data backups need to be maintained on a continuous basis.
- f) The data backup element of this policy applies to all staff and third parties who use ICT devices connected to the CENTLEC network or who process or store information owned by CENTLEC (SOC).
- g) All users are responsible for arranging adequate data backup procedures for the data held on ICT systems assigned to them.



- h) Backups should comprise of all the systems in the CENTLEC environment as stated in the backup procedure documents.

3. TIMING FOR DATA BACK-UP

Full backups of critical systems shall perform nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

4. RESPONSIBILITY FOR DATA BACK-UP

The IT department manager shall delegate a member of the IT department to perform backups. The delegated person shall also be responsible for testing backups and test the ability to restore data from backups on a monthly basis.

Those in charge of collection of data held either remotely on a server or on the hard disk of a computer, should consult the entity's system administrator or Information Systems Services about local back-up procedures.

5. BEST PRACTICE BACK-UP REQUIREMENTS

All backups must be executed in conformity with the following best practice requirements:

- i. All data, operating systems and utility files must be adequately and systematically backed up (ensure this includes all patches, fixes and updates);
- ii. Records of what is backed up and to where must be maintained;
- iii. Records of software licensing should be backed up;

- iv. At least three generations of back-up data must be retained at any one time (grandfather/father/son);
- v. The backup media must be precisely labelled, and accurate records must be maintained of backups done and to which back-up set they belong;
- vi. Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site; and
- vii. Regular tests of restoring data/software from the backup copies should be undertaken, to ensure maximum safety and security of the system.

6. DATA AND SYSTEMS TO BE BACKED-UP

Data to be backed up include the following information:

- a) User data stored on the hard drive.
- b) System data
- c) Backup date

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

- a) Active Directory
- b) Mail server
- c) Intranet web server
- d) Vending database servers
- e) Vending web servers
- f) Website server
- g) Solar Server
- h) Payday Server
- i) Mimic Server
- j) Digsilent
- k) Reticmaster

- l) Bently
- m) Historian

All other servers connecting all the users

7. TYPES OF BACK-UPS

There are quite a number of backup types and terms used when it comes to backups of digital content. CENTLEC (SOC) Ltd will use an incremental type of data backup. This therefore means that only a backup of all changes made since the last backup is made. The last backup can be a full back up or simply the last incremental backup. At the outset, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

Incremental data back-up will be performed for the following:

- Virtual machines (VMs); and
- Physical Databases.
- Physical Servers
- Data Storage

The incremental backup must be maintained on a daily basis for replication between the main site and disaster recovery side.

8. BACK-UP MEDIA

In terms of this policy, backups will be performed with an objective to achieve the following two distinct purposes:

- a) To ensure data recoverability after its loss, be it by data deletion or corruption; and
- b) To enable recovery of data from an earlier time for reference sake or any other purpose.

For this reason, CENTLEC (SOC) Ltd shall use External Hard Drives (EHD) as its primary back-up media.

The advantages of this medium as preferred secondary data storage include the following:

- a) recording capacity,
- b) price per unit of storage,
- c) write latency; and
- d) product lifetime

Other than the EHD, the company may also use other back-up media, including, but not limited to:

- CDs "Compact Disks"
- DVDs "Digital Virtual Disks"
- Memory sticks;
- Blue-ray discs;
- Backup tapes;
- Cloud backup;
- Combination of media, etc

Though backups popularly represent a simple form of disaster recovery, and should be part of a disaster recovery plan, backups should not alone be considered disaster recovery. One reason for this is that not all backup systems or backup applications are able to reconstitute a computer system or other complex configurations such as a computer cluster, active directory servers, or a database server, by restoring only data from a backup.

Every backup arrangement should include dry runs that validate the reliability of the data being backed up. It is important for those who are charged with information security of the company to recognize the limitations and human factors involved in any backup arrangement so as to limit any potential loss of critical data.

9. ARCHIVES

Archives of critical data shall be made every year and achieved for 5 years. Where appropriate, ICT services should ensure that archives are executed, managed and maintained in accordance with the National Archives Act (43 of 1996).

10. RESTORATION

Users that need files restored must submit a request to the IT Services desk. 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. The restore test must happen on a quarterly basis to test all backups.

11. ERASURE AND DISPOSAL OF BACKUP MEDIA

When the CENTLEC (SOC) Ltd determines that its computer or electronic storage media should be redeployed, discarded or dispose-off, one or more of the following techniques shall be used:

11.1 Erasure and Disposal Techniques

- a) **Wiping:** Wiping is a process of overwriting the space where files are located with random data using a wiping programs. Read/writable media should be “wiped” using a program / utility approved by ICT services.
- b) **Degaussing:** Degaussing is the erasure of information through the use of a very strong magnet. This technique may be generally used for erasing of magnetic media such as tapes and floppy disks.
- c) **Physical Destruction:** Certain media can be read many times but can only be written once. These media cannot be overwritten. Sometimes the media are defective and can no longer be used for retrieval or storage. In each of these cases the media should be physically destroyed. Any storage media

can be physically destructed / destroyed through burning, crushing or smashing.

In order to be effective, some of these techniques may necessitate a knowledgeable and competent person to ensure the storage media is appropriately erased. Therefore if any of the managers within the ICT services cannot ensure erasure or disposal of the media, a competent external service provider who can carry out the appropriate activity and demonstrate that they have succeeded shall be sourced.

11.2 Media under Warranty

Many hard drives are purchased with a warranty period. When devices fail during the warranty period, the vendor normally requires the return of the defective drive before a warranty replacement is provided. In most instances, warranty return of a defective drive includes all the data, documents and information stored on the drive prior to the fatal problems. Since sensitive data could potentially be exposed on a warranty returned defective drive, therefore, in instances where the warranty requirements includes data or information stored on the defective drive, the CENTLEC (SOC) Ltd shall instead resort to physical destruction instead of returning the drive to the vendor.

11.3 Important considerations

Regardless of any backup technique used, data should be available.

11.4 Audit Trail


ICT Services should maintain a log document of all media that have been erased and / or disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), erasure, destruction or disposal method used such as sold or crushed. The disposal software for the data on the hard drive must be used to ensure the completeness of the data disposal.




12. REVIEW AND APPROVAL

This policy and underlying strategies will be reviewed at least annually, or as necessary, to ensure its continued application and relevance.


Revised by:

Signed: 
Manager: Information Management
Date: 22 / 05 / 2023

Supported by:

Signed: 
Act Executive Manager: Engineering Retail
Date: 22 / 05 / 2023

Approved by:

Signed: 
Chief Executive Officer
Date: 22 / 05 / 2023