Letaba TVET College

BACKUP POLICY

TABLE OF CONTENTS

AMENDMENT AND APPROVAL RECORD

Amendment No.	Amendment description	Originator	Approved By	Date

Name of TVETC: LETABA		
Internal Audit Charter		
Unit: Corporate **Responsibility : Accounting Officer**		
_____ **Prepared and submitted by the Accounting Officer to Council** **Date:** _____	_____ **Authorised by Council** **(Signed by Chairperson obo Council)** **Date:**_____	**Implementation Date:** Date:_____

1. APPLICABLE LEGISLATIVE FRAMEWORK AND BEST PRACTICES

Key principles contained in the following legislation were applied to develop this policy:

a) CET Act No.16 of 2006 (as amended);
b) Public Finance Management Act, 1999 (as amended) (PFMA);
c) National Treasury Regulations of March 2005;
d) Electronic Communications and Transactions Act, 2002.

2. INTRODUCTION

Information security is becoming increasingly important to the College, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the College's ICT systems, data and infrastructure are protected from risks such as unauthorized access, manipulation, destruction or loss of data, as well as unauthorized disclosure or incorrect processing of data.

The Backup procedure is responsible for ensuring that all College data stored on approved systems within the College environment is recoverable in the event of accidental loss or damage.

3. PURPOSE AND OBJECTIVE

The purpose of this document is to provide guidance to the staff of the ICT Team to the processes that should be followed in order to ensure that the intellectual property of Letaba TVET College could be properly secured and recovered in the event of a failure. This document also guides the ICT Team to ensure that set standards are followed in the management of data backups.

It also seeks to ensure that Letaba TVET College adheres to all relevant laws governing the safeguard of its data (Electronic Communications and Transactions Act, 2002.)

4. SCOPE

The information that is contained in this policy has been developed for the sole purpose of providing a directive for managing and monitoring backups, backup media, the transport thereof and identifying certain responsibilities for these tasks.

The policy is applicable to Letaba TVET College and any applicable information for the other Sites will be specified accordingly**.**

The following data must be copied kept in a safe location.

- Coltech student data
- Coltech finance data
- Coltech Asset data
- Coltech user data
- Pastel Evolution finance data
- Student exam data.
- VIP payroll data
- Critical installed software
- Active directory data

5. DEFINITION, ACRONYMS AND ABBREVIATIONS

For the purpose of this policy, unless the context indicates otherwise, the following definitions acronyms and abbreviations are set out for the terms indicated:

5.1. Definitions:

5.1.1. “Accounting Officer” – is the College Principal

5.1.2. “Act” means: the Continuing Education and Training Act, 2006 (as amended).

5.2. Abbreviations:

5.2.1. DVD – Digital Versatile Disc

5.2.2. HD – Hard Drive

5.2.3. RAID – Redundant Array of Independent Disks

5.2.4. NAS – Network Access Storage

5.2.5. SQL – Sequential Query Language

5.2.6. MIS - Management Information Systems

5.2.7. TVET – Technical and Vocational Education and Training

5.2.8. EMIS – Education Management Information System

5.2.9. ICT – Information and Communications Technology

6. GOALS

6.1. To ensure that all backups across the College are well coordinated, effectively managed and responsive.

6.2. To provide timely, accurate, clear, objective and complete information about the backup procedures.

6.3. To ensure different backup levels are made regular to prevent data lost due to fire, theft, vandalism and virus infections.

6.4. To ensure that backups that were made is successful and recoverable.

6.5. To keep backups safely, securely and on more than one location

7. BACKUP TECHNOLOGY.

7.1. The Server is using RAID 1 Technology to keep data in synchronization on two hard drives.

7.2. The Network Assisted Storage device (NAS) is using RAID 1 Technology to keep data in synchronization on two hard drives.

7.3. Full data backups is made of the SQL data to make data recovery quicker.

7.4. Full data backups is made of Software.

7.5. Emails received are stored on the Service Provider Server for 14 days.

8. BACKUP FREQUENCY AND LOCATION

Backups are made according to the Grandfather, father and son principal. Grandfather backups are made yearly. Father backups are made monthly and son backups are made daily. Full backups are made of the SQL server data to make data recovery quicker and easier. Backup sets are tested on the MIS computer.

Backup	Frequency	Location	Responsibility
Coltech data	Daily, Monthly, Yearly	Server, NAS drive, MIS computer, Microsoft One drive cloud – Johannesburg data center.	Automated. MIS
Pastel evolution	Daily, Monthly, Yearly	Server, NAS drive, MIS computer, Microsoft One	Automated. MIS

		drive cloud – Johannesburg data center.	
Management documents	Monthly	DVD, External HD	Employee
Staff member documents	Monthly	DVD, External HD	Employee
Critical software	Once	DVD, External HD	MIS

9. BACKUP STORAGE

9.1. Backups are stored onsite and offsite. The backups are encrypted by using Advanced Encryption Standard (AES128).

9.2. Offsite locations are located on premises but in different building in a strong room.

9.3. Backups are also stored off premises in Microsoft One Drive – cloud service with the data center located in Johannesburg +- 400km from Letaba TVET College.

10. PROCEDURES

10.1 Student, Staff and Financial system data.

10.1.1. Daily backups

Daily backup of the SQL server must be made automatically in the evenings using the day of the month number. This will result in detailed backup kept with history of one month. The backups is transferred automatically to the Network assisted storage device. This is done by using a scheduling program to automate the backup process. A copy of the daily backup will also be copied to the cloud storage facility. A confirmation email is sent to MIS.

10.1.2. Monthly backups

Monthly backup of the SQL server must be made automatically in the evenings using the month name. This will result in backup kept with history of each month for a period of one year. The backups is transferred automatically to the Network assisted storage device. This is done by using a scheduling program to automate the backup process. A confirmation email is sent to MIS.

Manager and Staff is responsible to make their own monthly backups and keep it safe and secure.

10.1.3. Yearly backups

Yearly backup of the SQL server must be made automatically in the evenings using the Year number. This will result in detailed backup kept with history of each year. The backups is transferred automatically to the Network assisted storage device. This is done by using a scheduling program to automate the backup process. A confirmation email is sent to MIS

Data Retention periods

Backup Type	**Retention**
Daily	1 Month
Monthly	12 Months
Yearly	10 Years
Cloud storage	Only latest full backup – due to space and bandwidth consumption.

10.2. Student Exam Data

At the end of an exam backups should be made by a staff member that will move a snapshot of the current data from the class room server to a standalone computer. The staff member will then create a CD or DVD with the backup files. The CD or DVD must be labeled with the relevant subject information, exam date and stored in a safe and secure location. The CD or DVD must be accompanied with the seating plan during the exam, with the exam date, student ID and correlating computer number indicated.

When a CD or DVD was created the staff member must verify that the data is present on the disk.

Multisession CD or DVD will be allowed.

Data Retention period: 3 Years

10.3. Student Stored Data

Lecturers must make backups of student work and assignments every 30 minutes to limit work lost in case of a disaster.

Data Retention period: One exam cycle.

10.4. Management Documents

The Deputy Manager ICT and EMIS Manager are provided access to the NAS device to make backups of critical documents and files. It is their responsibility to make the backups. Incremental or differential backups can be done.

10.5. Staff Documents

Staff member should ensure that they make weekly backups of important documents and ensure that the backups are kept safe and securely.

10.6. Critical Software

The ICT unit should ensure that critical and important software is be stored in a safe and secure location.

11. BACKUP SOFTWARE

Reliable backup software must be used to create backups. The software must be able to move and compress data to be stored. The software must be user friendly and automate most of the backup processes.

12. BACKUP MONITORING AND TESTING

12.1. It is the responsibility of the Deputy Manager ICT and EMIS Manager to monitor the status (success or failure) of the backup schedules to ensure that any problems that have been picked up are detected as part of the daily server maintenance tasks.

12.2. Should any issues be identified it should be raised and the fault investigated in order to rectify anything that could cause the backups to fail.

12.3. It is also important to monitor the capacity used on storage devices before the storage device run out of space

12.4. The configured retention period of the backup logs which shows the failures and successes on the Backup will be kept for One year.

13. MANAGING BACKUP FAILURES

13.1. When a backup failed the cause of failure must be investigated and identified.

13.2. The failure and repair should be recorded in the event register.

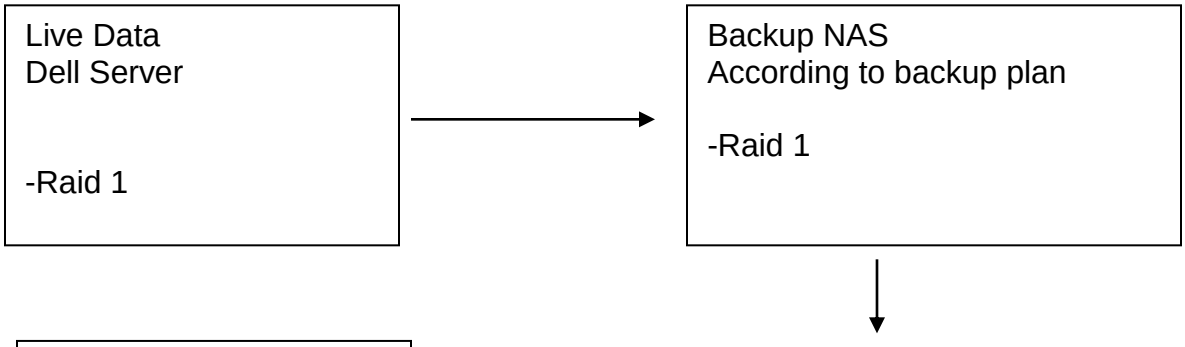
13.3. A manual backup must be made and tested monthly.

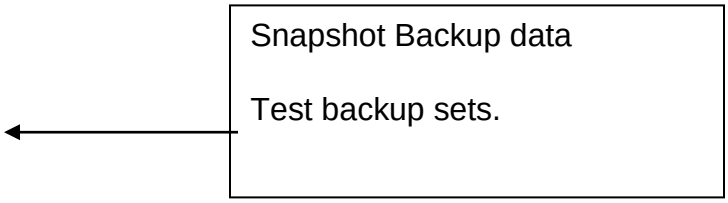
13.4. Where transactions were not committed. Instructions must be given to end users to re-capture the transactions.

14. BACKUP TESTS

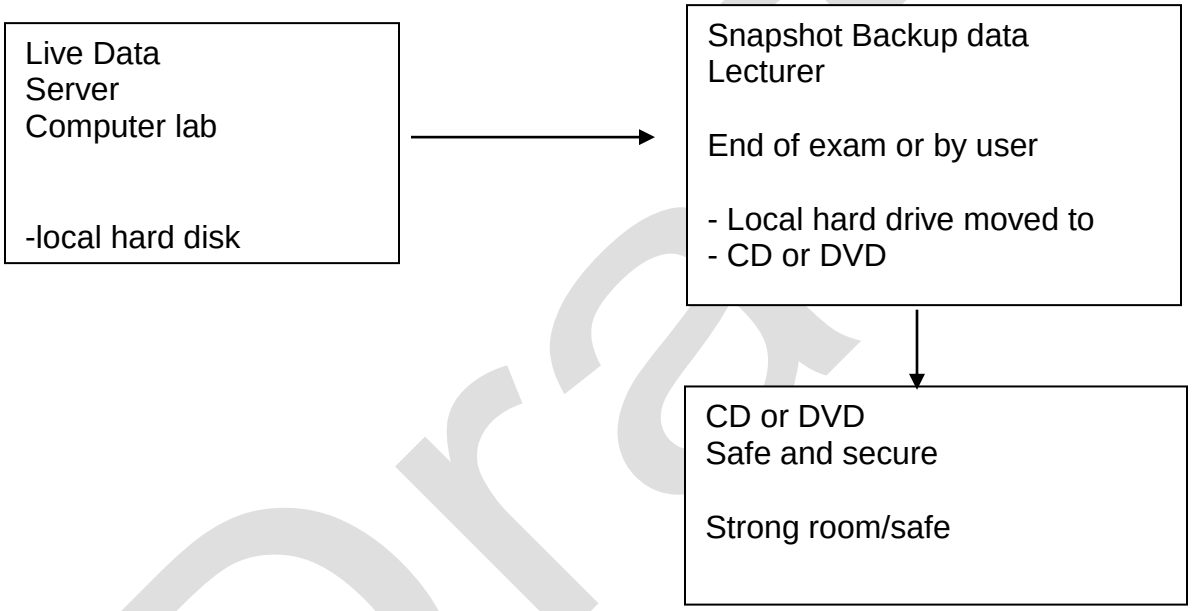
SQL backups must be restored and tested on an external system to ensure that the backups is recoverable. The test should be done at least once a month and the success of the backup recorded in a backup restore register.

Tzaneen Coltech Backup





Student Exam data6



15. APPROVAL

This policy shall be effective from the date of council approval and shall be reviewed after 3 years, with annual inputs.