

Business Owner:	Organisation Support & Development
Document Title:	Backup and Restore Policy
Document No.	ICT027/B&R/V3/24
Source:	ETBI V23
Approved By:	Chief Executive LWETB
Noted by:	LWETB Board
Date Noted:	November 2024

Longford and Westmeath Education and Training Board ICT Backup and Restore Policy

Contents

Contents	2
1. Introduction	3
1.1 Purpose of this Document	3
1.2 Scope and Constraints.....	3
1.3 Definitions.....	3
2. Backup and Restore Policy / ICT responsibility	3
3. User’s responsibilities	5
4. Enforcement	5
5. Policy Review and Continuous Improvement	5
6. Ownership and Approval	5

1. Introduction

1.1 Purpose of this Document

The Longford and Westmeath Education and Training (LWETB) Backup and Restore Policy should be read in conjunction with all other ICT policies to ensure required security standards are adhered to. The purpose of this policy is to define the activities associated with the provision of data backup and recovery plans and programs that protect LWETB information systems, networks, data, databases, and other information assets.

1.2 Scope and Constraints

The scope of this backup and recovery policy is all information technology systems, software, databases, applications, and network/security resources needed by LWETB to conduct its business.

1.3 Definitions

A full range of definitions is available in the ICT Security Frameworks Policy available [here](#).

2. Backup and Restore Policy / ICT responsibility

ICT will ensure that regular backups are performed in line with Asset Owner requirements as appropriate.

The interval/frequency between backups should be linked to the sensitivity, impact of loss, corruption or non-availability of the data as identified by the asset owner as appropriate. All backup and archive media must be stored in a suitable environment according to the value of the information.

2.1. Backup

The following must be considered when making backups:

- The need to keep backup copies and associated procedures in a different place from where the systems which process such information are found.
- The need to encrypt information with backup.
- The need to label and inventory backups in keeping with the classification of the contained information.
- The need to encrypt back-up data where the original information is encrypted. The encryption can be through the backup copying system, or the information can be stored in encrypted format. The encryption keys and associated programmes must be stored separately so that the data can be retrieved using the encryption information if necessary.
- The need to check backup copies periodically and on a rota basis abiding by predefined testing schedules, using a verification tool or retrieving part of the set, in order to guarantee that the copies are available when needed.
- Backup copies should be made in such a way that they permit individual file/folder retrieval as well as entire system retrieval from the system and the information processed.
- Backup copy-making procedures should be automated, making the task easier for operators and preventing possible errors in copy handling.

- Wherever necessary, a backup copy of the information and copy of the retrieval procedure should be kept in a different place from that where the data processing systems are found. Such location should comply with all the security measures applied to the original location or should feature elements which guarantee the integrity and retrieval of the information, making its recovery possible.
- The correct definition, running and application of the backup copy and retrieval procedure should be checked periodically. This verification should be carried out at least every 6 months.

2.2. Retrieval

- The recovery of information from backup copies must be authorised by the data owner. The backup system installed should not depend on itself for its own retrieval.

Where backups are created, the following information should where possible be included in a **documented and formalised backup and recovery plan**:

<p>General Information</p>	<ul style="list-style-type: none"> • the person(s) responsible for making the backup copies and for their custody • the frequency of backup copies • the number of copies • the type of backup (complete or differential/incremental) • maximum storage times (expiry dates) and whether it is necessary to delete the information once expiry date is reached (as well as the type of destruction required) • acceptable minimum times for information retrieval
<p>Backup Information</p>	<ul style="list-style-type: none"> • register(s) of the copies made • retrieval procedures
<p>Recovery Information</p>	<ul style="list-style-type: none"> • recovery actions • the people executing the process • the authorisation for recovery • the information restored • the reason for recovery • the validation processes associated with the operation and the acceptance on the part of the data owner of the recovered information or system. This should guarantee the reconstruction of the information in the same status as it was at the time of the loss or destruction, according to the retrieval times established and agreed with its [asset owner].

- The data backup and recovery plan must be kept up to date that reflects the changes to the updated environment.

3. User's responsibilities

Users should notify the ICT helpdesk / asset owner immediately upon discovering a possible need to restore data.

Users should ensure all information is stored appropriately to ensure work related information is backed up and can be restored when required.

Users must store work information in the appropriate location as identified by ICT support/ Line manager to facilitated successful backup of information.


4. Enforcement

Individuals found to be in breach of this policy may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to be answered by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

5. Policy Review and Continuous Improvement

This document was reviewed in line with best practice, and has been approved by senior management, who are committed to continually improving the protection of all LWETB Information Assets and the protection of personal data where LWETB is a controller or processor. This document will be reviewed at least once every two years by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within LWETB. The date of implementation is the date of Chief Executive approval.

6. Ownership and Approval

OWNER	DATE	SIGNATURE
Organisation Support & Development Director	Nov 4, 2024	 Charlie Mitchell (Nov 4, 2024 16:58 GMT)
AUTHORISED/APPROVED BY	DATE	SIGNATURE
Chief Executive	Nov 5, 2024	