

<b>Business Owner:</b>	<b>Organisation Support &amp; Development</b>
<b>Document Title:</b>	<b>Asset Management Policy</b>
<b>Document No.</b>	<b>ICT030/AM/V2/23</b>
<b>Source:</b>	<b>ETBI</b>
<b>Approved By:</b>	<b>Chief Executive LWETB</b>
<b>Noted by:</b>	<b>LWETB Board</b>
<b>Date Noted:</b>	<b>14/11/2023</b>

# Longford and Westmeath Education and Training Board

## ICT Asset Management Policy

## Contents

<b>1.</b>	<b>Introduction .....</b>	<b>3</b>
1.1.	Purpose of this Document .....	3
1.2.	Scope and Constraints.....	3
1.3.	Definitions .....	3
<b>2.</b>	<b>Asset Management Policy/ICT responsibility.....</b>	<b>3</b>
2.1.	Asset Owner Responsibilities .....	4
2.2.	User responsibilities.....	4
2.3.	Environmental Controls .....	4
2.4.	Risk Assessment Procedures.....	5
<b>3.</b>	<b>Enforcement.....</b>	<b>6</b>
	<b>Ownership and Authorisation .....</b>	<b>6</b>
	<b>Revision History.....</b>	<b>6</b>

## 1. Introduction

### 1.1. Purpose of this Document

The Longford and Westmeath Education and Training Board (LWETB) ICT Asset Management Policy should be read in conjunction with all other ICT and relevant policies. This policy documents the approach to ICT asset management to ensure there are appropriate controls and report structures in place to manage LWETB owned ICT assets.

All users that have access to organisational information systems must adhere to the ICT asset management policy defined below in order to protect the security of LWETB data, protect and control computer systems and organisational ICT assets.

### 1.2. Scope and Constraints

The scope of this policy applies to all Users.

All forms of ICT assets are in scope, whether located on LWETB premises or not, including but not limited to:

- **Physical:** computer and communications equipment, mobile devices, other technical equipment (UPS, backup hardware, etc.).
- **Software:** application software, system software, development tools and utilities
- **Services:** computing and communication services, other technical services whether located on a LWETB premises or not.

### 1.3. Definitions

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

## 2. Asset Management Policy / ICT responsibility

The following controls apply to the general management of assets. There are two categories of assets being considered for this policy:

Asset: any hardware/software/service with a value from €0 – €5,000.

Significant Asset: any hardware/software/service with a value above €5,000.

- LWETB Corporate Services will keep an inventory of all ICT assets over €150 approx & any ICT asset which is capable of retaining LWETB data.
- All Assets must have a designated Asset Owner included in the Assets Register. This must be a LWETB employee, not a contractor or employee of a third party. The Asset Owner's roles and responsibilities are defined in Section 2.1.
- The ICT Asset Register should contain the following information in order to track assets;
  - a. Asset ID
  - b. Serial Number
  - c. Description (including model)
  - d. Type of asset
  - e. Owner
  - f. Department
  - g. Purchase Date
  - h. Supplier
  - i. Cost

- Corporate Service or ICT support will follow all LWETB asset disposal policy requirements, while also ensuring the following criteria are met:
  - a. Company assets which may contain LWETB data (e.g. all Storage devices), that are no longer used must be destroyed in such a way that it is impossible to recover information from them afterwards (e.g. Shredding, Degaussing or unrecoverable secure wipe).
  - b. For Damaged Media whereby it is not possible to destroy the data by logical means, then the media must be physically destroyed or rendered unreadable (e.g. shredding or degaussing).
  - c. An auditable record must be maintained of all hardware to be disposed of or destroyed.
- The person assigned to the asset will ensure physical security perimeters are in place and adequate to protect the areas where assets are located, while considering the total value of the assets contained and the potential environmental hazards of where the asset is being located.
- The presence of business-critical installations within a building should not be highlighted by the use of descriptive signposts or other displays. Where signposts or other displays are used, they should be worded in such a way that attention is not brought to the activity taking place within the building.
- Business critical areas must be secured, and access restricted to authorised people only.
  - a. Communications rooms /communications equipment - unless in lockable secure furniture;
  - b. Computer rooms;
  - c. Media stores.

## 2.1. Asset Owner Responsibilities

Asset Owner responsibilities focus on the following areas:

- Knowing who has access to an Asset and why. Ensuring that this access/use of the Asset is monitored.
- Understanding and addressing any risks to assets and ensuring any data loss incidents are appropriately managed.

## 2.2. User responsibilities

- Users are not permitted to modify or transfer an Asset tag in any way.
- Users must ensure they always act in a responsible manner when using LWETB equipment.
- Users must report any damage to equipment via email to Corporate Services immediately on [corporate@lwetb.ie](mailto:corporate@lwetb.ie).

## 2.3 Environmental Controls

- Computer equipment should be protected from electrical failures and other supply-related problems (water, ventilation, air conditioning etc.). Where high availability is required, electronic equipment should be safeguarded from the threat of disrupted electric power. Depending upon its criticality, this may require implementation of some or all of the following:
  - a. Provision of duplicate power feeds from alternative sub-stations;
  - b. Uninterrupted Power Supply (UPS);
  - c. Standby generator facilities where possible

UPS and standby facilities should where possible be tested and must provide sufficient capacity for the operational need.

- Where high availability is required or valuable assets could be damaged, alarms should be installed and connected back to a permanently manned position to enable detection of the following:
  - a. fire;
  - b. flood;
  - c. power failure;
  - d. failure of the Uninterrupted Power Supply (UPS);
  - e. failure of environmental equipment, (e.g. air conditioning);
  - f. Abnormal environmental conditions.

## 2.4 Risk Assessment Procedures

A risk assessment should be carried out on Significant Assets.

The following approach should be taken for the risk assessments of significant assets:

- Identify all Significant Information Assets.
- Identify corresponding assets owners.
- Identify risks to assets based on criteria such as Confidentiality, Integrity and Availability.
  - a. Confidentiality - risks to unauthorised access and misuse
  - b. Integrity - risks to unauthorised alteration
  - c. Availability - risks to unavailability for authorised users
- Identify corresponding risk owners - someone who is closely related to the process or operations where the risk has been identified.
- Analyse the identified risks and assess the likelihood and impact to the business if a risk were to materialise.
- Determine the risks levels - through categorisation such as low, medium, high. For instance, risks can be determined by factors such as business impact and level of occurrence (a risk with high impact and high level of occurrence would result in an overall high-risk level.)
- Prioritise the analysed risks for risk treatment. Risk treatment options include, but are not limited to:
  - a. Risk mitigation - reducing exposure to the effects of risks (patching, applying security controls, etc.)
  - b. Risk avoidance - removing and no longer using an asset with an identified risk.
  - c. Risk acceptance - accepting the risk and taking no further actions. This should be recorded in a risk register and is not a recommended approach unless the risk has been assessed and has a low risk level.
  - d. Risk transfer - moving/sharing risk responsibility with another entity (such as a third party, e.g. insurance company).

### 3. 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 answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

### 4. Policy Review, Approval and Continuous Improvement


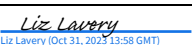
In line with best practice, this policy has been approved by senior management, who are committed to continually improving the protection of all LWETB Information Assets and the protection of personal data where LWETB is a controller or processor. This document will be reviewed at least annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within LWETB.

This document will also be reviewed in light of changes in legislation and guidance from sources such as Internal Audit, C&AG, the Department of Education, the Department of Further and Higher Education, Research, Innovation and Science and the Department of Public Expenditure & Reform, or on the issuing of circular letter or by the Chief Executive in response to business needs. The date of implementation is the date of Chief Executive approval.

### 5. Reference

ISO27001	NIST CSF	PCI-DSS

### Ownership and Authorisation

OWNER	DATE	SIGNATURE
Organisation Support & Development Director	Oct 31, 2023	 Charlie Mitchell (Oct 31, 2023 13:57 GMT)
AUTHORISED BY	DATE	SIGNATURE
Chief Executive	Oct 31, 2023	 Liz Lavery (Oct 31, 2023 13:58 GMT)

### Revision History

VERSION	DESCRIPTION	REVISION DATE	REVIEW DATE
ETBI	ETBI 2022	2023	Annually