Title	**LWETB Asset Protection Policy**
Date	26th May, 2020
Approved	Chief Executive LWETB
Noted By	LWETB Board (26th May, 2020)

LWETB
Asset Protection Policy

1. Purpose

The purpose of the IT Asset Protection Policy is to effectively ensure significant IT-Assets are appropriately managed and controlled.

Please note if there is anything in this Policy which is unclear or if you have any questions please contact ICT Support who will provide assistance.

2. Description

This policy applies to all staff, contractors and all who access and use LWETB IT systems with particular emphasis on the roles and responsibilities of the Data Owner.

3. Definitions

An **"IT Asset"** is defined as any system, service, device, or data owned or controlled by LWETB or that is utilised or accessed by LWETB staff, contractors, or partners. This can be any tangible or intangible thing that has value to LWETB and therefore must be protected.
An **"Asset Owner"** (sometimes referred to as a **"Business Owner",** or **"System Owner"**), is defined as the person with overall responsibility and accountability for the asset. The Asset Owner has responsibility for the asset's maintenance, use and security as appropriate. The Asset Owner must be a member of LWETB staff, not a contractor or employee of a third Party.
A **"Data Owner"** (sometimes referred to as the **"Information Owner"**), is defined by LWETB's Data Handling Policy as the "Individual or group responsible for classifying data and generating guidelines for its lifecycle management. These are usually the officers responsible for the initial collection/input and use of the data. The Data Owner must be a member of LWETB staff, not a contractor or employee of a third Party.
"Must", or **"required"** or **"shall"**, refer to an absolute requirement of the policy.
"Must not", or **"shall not"**, refer to statements which are an absolute prohibition of the policy.
"Should", or **"recommended"** refer to a statement that should be applied. In certain circumstances, there may exist a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.
"Should not", or the phrase **"not recommended"** mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

1. All physical IT assets to the value of over 300 euro must be captured on the LWETB Asset Register (e.g. Computers, Servers, Switches, Laptops etc.)

2. All IT assets must have a designated Data and/or Asset Owner. This must be an LWETB employee, not a contractor or employee of a third Party.

3. The Asset and/or Data Owner must define the security requirements, ensuring the continued operation, confidentiality and integrity of the asset and ensuring all security risks are appropriately managed on the systems, service or information for which they are responsible.

4. The Asset and/or Data Owner must ensure the assets they are responsible for have an appropriate continuity strategy, business continuity and resumption plan(s).

5. The Asset and/or Data Owner must ensure appropriate security risk assessments are undertaken to check that the assets are sufficiently protected and are in line with security policy. To design cost effective security measures, it is recommended that a risk assessment is carried out on assets, to establish the likely threats to the asset(s) and consequences of interference, damage or loss to the assets.

6. The Asset and/or Data Owner must ensure all Assets for which they are responsible are compliant with LWETB security policies including, for example, Data Protection Policy, Password Policy, Logical Access Policy, Anti-virus and Malware protection policy, Partnering policy.

7. The Asset and/or Data Owner must ensure security compliance checks of systems are completed to validate compliance with the policy. These should include checking:

- Anti-Virus is functional and updating (as per anti-virus policy)
- Technical controls to enforce operating system password policy are in place (as per password policy)
- Audit logging of privileged access and log-on/log-off activities are being captured (as per Logical Access Policy)
- Systems are patched and up to date (both operating systems and software). All software and operating systems must be updated with the latest security patches recommended by the manufacturer. Priority should be given to the installation of those patches which solve the most serious vulnerabilities in the systems with greatest exposure and risk, taking into account criticality.
- All software is authorised and licensed appropriately

8. To deal with security mechanisms and measures, the Data Owner may choose to delegate the security tasks, in full or partially, to an Asset Handler or other

representative (e.g. LWETB Help Desk, or third party security). This delegation does not exempt the Data Owner from their responsibility and they must make sure that the delegated jobs have been carried out correctly and corrective actions taken; they remain accountable. In addition, where such delegation takes place, this must be by written mutual agreement.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisational Support and Development	Revisions and updates to the Policy
LWETB Senior Leadership Team	Review
LWETB Chief Executive	Approval of the Policy
Asset Owner	Accounting for the location of the Asset at all times.
Data Owner	Responsible for implementation of the Policy
Internal and external audit	Monitoring and reporting compliance with the Policy

6. Related Documents

- Password Acceptable Usage Policy
- Partnering Policy
- Remote Access Policy
- Logical Access Policy
- Encryption Policy
- Anti-Virus and Malware Protection Policy
- End User Policy