lwetb
Bord Oideachais agus Oiliúna an Longfoirt agus na hIarmhí
Longford and Westmeath Education and Training Board

Title	**LWETB Partnering Policy**
Date	9th March, 2020
Approved by	LWETB Meeting 9th March, 2020
For Review By	LWETB Board

LWETB
Partnering Policy

1. Purpose

It is envisaged that LWETB will partner with selected parties to provide ICT services. As security levels vary from one organisation to another it is important to ensure that a minimum level of protection is defined to protect LWETB.

LWETB requires that all partners meet an effective level of information security that is aligned with existing security policies (e.g. remote access, data handling and incident response policies). All partners must be made aware of their responsibilities and ensure that adequate protection is in place relative to the service being provided.

Special security issues that relate to partnering include the following:

- The use of LWETB personal data.
- Access to LWETB systems.
- Any LWETB classified data stored on partner systems that may be compromised should it be stolen or lost.

The purpose of this policy is to ensure that effective measures are in place to limit any exposure to LWETB.

2. Description

This policy applies to all LWETB partners who provide ICT services: for example, hosting a service, developing an application or providing technical support services. This policy is not dependent upon the service being delivered onsite and is applicable in all cases.

It is the responsibility of the Data Owner - LWETB - to ensure the policy is implemented with all partners who process their data.

3. Definitions

“Partner” is defined as any organisation providing a service to LWETB. This service may be on or off site.
A **“Data Owner”** (sometimes referred to as a “**Business Owner**”, “**System Owner**”, or **“Asset Owner”**), is the person with overall responsibility for the system or service and in particular the data held. This should be the Manager or Head of function that commissioned the system or service and/or that owns the processes and data supported by the system or service. The Data Owner must be a LWETB staff member, not a contractor or employee of a 3rd Party.
“Must”, or the terms "**required**" or "**shall**", refer to an absolute requirement of the policy.

"**Must not**", or the phrase "**shall not**", refer to statements which are an absolute prohibition of the policy.
"**Should**", or the adjective "**recommended**" refers 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.

4. Requirements

The following security controls apply:

1. The partner should have their own defined security policies, which should be supported by documented procedures, and be approved by LWETB ICT Support.

2. All partners engaged in the exchange of information must be compliant with all LWETB policies including, but not limited to, the Data Protection policy, Remote Access policy, Encryption policy and logical access policy.

3. A signed agreement/contract must be in place between LWETB and all partners.

4. The following criteria must be included in all agreements:

- A statement of compliance with LWETB security policies.
- The contract must include a suitable Non-Disclosure Agreement (NDA), if applicable e.g. personal information is exchanged or LWETB intellectual property is divulged. LWETB have a standard NDA which can be obtained from the Director of Organisational Support & Development on request.
- Security responsibilities must be clearly defined including the security controls applied to LWETB data. **This is also a legal requirement where personal data may be processed**.
- A notification procedure and security incident management procedure.
- Right to audit and monitor compliance with the security requirements and controls of the agreement.
- Return or destruction of the information on completion of the agreement.
- Change management procedure.
- Service level and acceptable parameter indicators.

5. When a system is being developed by a partner, the following points must also be in the written contract:

- The ownership, intellectual property rights and licensing agreements of the developed software must be clearly defined.
- Application security requirements must be clearly defined.
- The quality and security of the delivered software should be guaranteed by contract, making the third party responsible for any damages incurred by LWETB due to shortcomings in the software.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisational Support & Development	Revisions and updates to the policy
LWETB Management Team	Approval of the Policy
Data Owners	Ensuring implementation of policy.
Internal and external audit	Monitoring and reporting compliance with the policy
Partners	Compliance with the terms of the policy

6. Related Documents

- Data Protection Policy
- Password Acceptable Usage Policy
- Remote Access Policy
- Asset Protection Policy
- Logical Access Policy
- Encryption Policy
- Anti-Virus and Malware Protection Policy
- ICT Acceptable Usage Policy