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

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

LWETB Remote Access Policy

1. Purpose

Remote access to LWETB systems will be required for a variety of purposes. This remote access must be controlled to ensure that LWETB's systems and data are not placed in jeopardy. The purpose of this policy is to ensure the correct balance between access and the potential risk posed to systems and data, and to ensure the continued availability and confidentiality of these systems and data.

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

The policy applies to:

- All staff who have remote access to LWETB IT systems.
- All others who have remote access to LWETB IT systems.

3. Definitions

"Remote Access" is defined as access to LWETB's systems from any non-LWETB network or from the Internet whether on or off LWETB infrastructure.
"Must", **"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 be 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 **"not recommended"** mean the specified behaviour should not be performed. There may be 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 so described.

4. Requirements

1. The same security policies apply to remote workers as to office-based personnel. When working remotely all applicable policies and in particular Data Protection, Encryption and ICT Acceptable Usage policies must be complied with. For example, if working on "LWETB Restricted" information, all paper waste must be securely destroyed and in accordance with the Data Protection Policy.

2. Remote access to LWETB systems must be for a specified and legitimate purpose.

3. Remote access to LWETB systems must use an approved remote access technology. Currently approved remote access technologies are:

a. Approved Virtual private network (VPN)
b. Microsoft UAG Portal Access
c. Forticlient Remote access

If the remote access mechanism is not detailed above, then it is not an approved method and must not be used. This includes all other forms of remote access. Specifically, software which establishes outbound connection to 3rd party sites, and can then be used to access a user's desktop remotely must not be used. In the event of any doubt as to the application of this clause, the guidance of the ICT Support should be sought.
(Access of third party cloud based systems are accessible using the agreed security protocols between LWETB and the relevant third party provider.)

4. Organisations or individuals wishing to implement non-standard remote access must obtain prior approval from LWETB ICT Support.

5. All individuals are responsible for safeguarding the remote access credentials granted to them and making sure that unauthorised individuals do not use them. These credentials may consist of username and password combinations, digital certificates or other software or hardware. Users must not provide their password to any other person or entity, or use devices available to the public, e.g. in airports and hotel receptions, or log on using public wifi hotspots.

6. If you remotely use LWETB's systems then you must ensure that the following are in place:

- A strong password which conforms with LWETB's password policy.
- Your password is not based on a dictionary word.
- You have not shared your password with anyone else.
- You must not attempt to log on as another individual even if they have given you credentials.
- No group (or generic) accounts are used for remote access.
- The system you are using for remote access has sufficient protection in terms of anti-virus, malware protection and has been updated with the latest operating system patches.
- Caution should be exercised when accessing LWETB's systems remotely, especially from networks that may be insecure., e.g. public wifi.

7. Remote users must not bypass security mechanisms to remain logged onto systems for longer periods than those configured by LWETB ICT Support.

8. When remote access is provided to any system, access should be granted on the principle of “least-privilege”. Specifically, users should not be granted access to systems or functions to which they do not need access.

9. Where possible any LWETB personal data and/or LWETB sensitive information accessed remotely should not be stored on smartphones (or other mobile devices) or must be protected in accordance with the additional policies listed below.

10. Any suspicious behaviour or security incidents (for example if you suspect your network account has been compromised) must be reported to the LWETB ICT Support and to your Manager immediately.

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
All End-users	Responsible for complying with and implementation of the Policy
Internal and external audit	Responsible for complying with and implementation of the Policy
LWETB ICT Support	Tracking of calls related to Security Incidents

6. Related Documents

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