Business Unit	**Corporate Services - ICT**
Document Title	**LWETB Remote Access Policy**
Document No.	**ICT014/RA/V2/22**
Approved By	**Chief Executive LWETB**
Date Approved	**12/12/2022**
Noted By	**LWETB Board**
Date Noted	**20/02/2023**

Longford and Westmeath Education & Training Board

Remote Access Policy

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

Contents

1 Introduction 2

1.1 Purpose of this Document 2
1.2 Scope and Constraints 2
1.3 Definitions 2

2 Remote Access Security Policy 2

2.1 ICT Technical Standards 2
2.2 Third Parties' Responsibilities 3
2.3 User Responsibilities 4

3 Enforcement 5

4 Review and Implementation 4

5 References 4

1 Introduction

1.1 Purpose of this Document

The Remote Access policy is defined in the Longford and Westmeath Education & Training Board (LWETB) ICT Security Framework Policy and should be read in conjunction with all other ICT policies to ensure that required security standards are adhered to. This policy refers to the use and administration of the remote working environment utilised by LWETB to facilitate the processing of Corporate Data by employees. All employees who are required to interface with the system must read and adhere to all aspects of the policy.

This policy covers two aspects of remote access:

1. Internal User access.
2. External User access on an AD-hoc basis and in accordance with agreed SLA.

1.2 Scope and Constraints

This policy applies to all users referred to in the definitions section of the ICT Security Framework Policy. It covers any computing devices or data storage devices connected to LWETB technology infrastructure using any connection method. This policy covers all mobile computers or devices used to store Corporate Data. This includes but is not limited to desktop computers, laptops, smart phones, memory sticks, removable media, servers, networking equipment. This policy is effective as of the issue date and does not expire unless superseded by another policy.

1.3 Definitions

A full range of definitions is available in the ICT Security Framework Policy.

2 Remote Access Security Policy

2.1 ICT Technical Standards

1. Remote access for LWETB users must be configured to lock out after five (5) minutes inactivity
2. Configuration standards must be developed for all remote access system components:
   a) These standards must address all known security vulnerabilities and be consistent with industry-accepted system hardening standards
   b) System configuration standards must be updated as new vulnerability issues are identified
   c) System configuration standards must be applied when new systems are configured and verified as being in place before a system is installed on the network. Access must be granted on a basis of “minimum-rights” and “need-to-know” along with appropriate expiry timelines
3. All users must be given their own unique account – generic accounts must not be used
4. Permanent remote access must only be available to LWETB users or third parties who have permanent access in accordance with their respective service level agreement.

5. Audit logs may be stored and available upon request
6. Authentication based exclusively on the source address of the users' system (IP Address, MAC Address etc) must not be used
7. Where possible, only necessary services, protocols, daemons, etc., may be enabled as required for the function of the system:
    - Where possible all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be removed
    - For services, protocols, or daemons considered to be insecure (*e.g.*, telnet, FTP), additional security features must be implemented
8. System security parameters must be configured to prevent misuse
9. The ICT Department will employ multiple methods, tools, and audit processes to monitor and assess whether security controls and measures have been implemented and are being followed
10. Where possible access must be provided to users in a Virtual environment and only provide access to the application required to perform their duties
11. Maintenance of remote access solution shall only be performed as agreed with LWETB
12. A list of authorisations for individual user remote access will be maintained for information security and audit purposes

2.2 Third Parties' Responsibilities

1. Remote access technologies used to access LWETB technology infrastructure by third parties must be configured to automatically disconnect sessions after five (5) minutes of inactivity.
2. Configuration standards must be developed for all remote access system components
    a) These standards must address all known security vulnerabilities and be consistent with industry-accepted system hardening standards
    b) System configuration standards must be updated as new vulnerability issues are identified
    c) System configuration standards must be applied when new systems are configured and verified as being in place before a system is utilized in the LWETB technology infrastructure.
3. Maintenance shall only be performed as agreed with LWETB
4. Where permitted, remote access for supplier maintenance or diagnostics purposes will be strictly controlled to protect the security of the system.
5. Security controls must be agreed and defined in a contract with the third party and must include an agreed method of access.
6. Any suspicious activity must be promptly reported to LWETB's Corporate Services, Director of OSD, or DPO.
7. All remote access to corporate data by third party suppliers must be agreed as part of a data sharing agreement by LWETB.
8. Where temporary remote access is required by a third party, it must be granted as follows:
    a) Access must be requested prior to attempting connection
    b) Must be deactivated or disabled immediately after each use

c) Only enabled from the LWETB end after manual intervention when the need arises
d) Have all remote diagnostic activity logged and audited
e) Have any login id's allocated for this purpose disabled when not in use
f) Access only to the system for which access was granted
g) The third party must not be able to detect other network based hosts;
h) All automatic disconnect configurations will be periodically validated

9. Third party organisations (customer or support organisations), shall only be provided with remote access on a temporary basis.

2.3 User Responsibilities

1. Only ICT/CS, approved secure remote access technologies, such as virtual private networks (VPN) may be used when accessing LWETB production systems
2. Remote access tools that establish outbound and always-up connections are not permitted unless ICT, via managers, approved [*e.g.* Team Viewer and Logmein *etc*].
3. Access to company data must only be carried out over secure sessions using approved encryption.
4. Remote users must be registered and authorised prior to using the service allowing connection to LWETB Corporate Data.
5. The use of LWETB remote access solution may require Multi Factor Authentication
6. Any suspicious activity must be promptly reported to LWETB's Corporate Services on corporate@lwetb.ie
7. Remote credentials (including any secure fob) must not be shared with anyone.

3 Enforcement

Individuals found to be in breach of this Remote Access Policy, may be subject to disciplinary action, up to and including contract termination or dismissal where appropriate. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User / responsible third party, the matter will be referred into the appropriate stage of the relevant procedure as appropriate to that User / responsible third party.

4 Policy Review, Approval and Continuous Improvement

This policy will be reviewed annually by the Senior Leadership Team in line with best practice, or 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. Along with commitment to continually improve 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 ensure alignment to appropriate risk management requirements and best practice for the management of remote access within LWETB. The date of implementation is the date of LWETB Chief Executive approval.

5 References

ISO27001	NIST CSF	PCI-DSS