City of Dublin Education and Training Board

Remote Access Policy

Document version	2
Drafted by	ETBI (ICT Group)
Responsibility for this policy in City of Dublin ETB	Director OSD and Head of IT
Reviewed by Senior Leadership Team (SLT)	12 October 2021
Approved by Chief Executive	12 October 2021
Noted by Board	21 October 2021
To be reviewed	1 year from date of approval by CE

Contents

1 Introduction 3

1.1 Purpose of this Document 3
1.2 Scope and Constraints 3
1.3 Definitions 3
1.4 Policy Review, Approval and Continuous Improvement 3

2 Remote Access Security Policy 4

2.1 ICT Technical Standards 4
2.2 Third Parties' Responsibilities 4
2.3 User Responsibilities 5

3 Enforcement 6

1 Introduction

1.1 Purpose of this Document

The Remote Access policy is defined in the City of Dublin ETB ICT 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 City of Dublin ETB 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. It covers any computing devices or data storage devices connected to City of Dublin ETB 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 This policy is effective as of the issue date and does not expire unless superseded by another policy.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 Frameworks Policy

1.4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, along with its commitment to continually improve the protection of all City of Dublin ETB information assets and the protection of personal data where City of Dublin ETB is a controller or processor.

This document will be reviewed annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of remote access within City of Dublin ETB.

2 Remote Access Security Policy

2.1 ICT Technical Standards

1. Remote access for City of Dublin ETB users must be configured to lock out after 15 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 City of Dublin ETB users or third parties who have permanent access in accordance with their respective SLA;
5. Audit logs may be stored for 12 Months and available upon request and reviewed as required;
6. Authentication based exclusively on the source address of the users' system (IP Address, MAC Address etc) must not be used;
7. Change-detection mechanisms (*e.g.*, file-integrity monitoring tools) may be implemented and configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files;
8. A risk assessment/data protection impact assessment should be performed and approved by the City of Dublin ETB prior to granting remote access to any third-party.
9. System security parameters must be configured to prevent misuse;
10. The IT 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;
11. Where possible access must be provided to users in a Virtual environment and only provide access to the application required to perform their duties;
12. Maintenance of remote access solution shall only be performed as agreed with City of Dublin ETB**.**
13. 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 City of Dublin ETB technology infrastructure by third parties must be configured to automatically disconnect sessions after 15 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 utilised in City of Dublin ETB technology infrastructure.

3. Maintenance shall only be performed as agreed with City of Dublin ETB.
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 City of Dublin ETB's IT Department.

   All remote access to corporate data by third party suppliers must be agreed as part of a data sharing agreement by City of Dublin ETB
7. 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 City of Dublin ETB 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;
8. Third party organisations (customer or support organisation), shall only be provided with remote access on a temporary basis.

2.3 User Responsibilities

1. Only IT department approved secure remote access technologies, such as virtual private networks (VPN) may be used when accessing City of Dublin ETB production systems
2. Remote access tools that establish outbound and always-up connections are not permitted unless IT department approved.
3. Access to company data must only be carried out over secure sessions using approved encryption. Reference Encryption policy for further information.
4. Remote users must be registered and authorised prior to using the service allowing connection to City of Dublin ETB Corporate Data.
5. The use of City of Dublin ETB remote access solution will require Multi Factor Authentication.
6. Any suspicious activity must be promptly reported to City of Dublin ETB's IT Department.
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.