

Access Control Policy

|  |  |
| --- | --- |
| Policy Area | Corporate Services |
| Version | 0.5 |
| Date | Created: March, 2023 |
| Monitored | Every three years or as required |
| Responsibility | ICT & Corporate Services Section |
| Approved | Senior Management |
| This policy document is an uncontrolled copy. Each staff member should consult StaffCONNECT for the latest version of this document. |

Contents

[1 Introduction 4](#_Toc142487127)

[1.1 Purpose of this Document 4](#_Toc142487128)

[1.2 Scope and Constraints 4](#_Toc142487129)

[1.3 Definitions 4](#_Toc142487130)

[1.4 Policy Review, Approval and Continuous Improvement 4](#_Toc142487131)

[2 Policy 4](#_Toc142487132)

[2.1 ICT Responsibility / User account creation and management 4](#_Toc142487133)

[2.2 ICT Responsibilities / Logical Access Security Controls (including Security Hardening) 6](#_Toc142487134)

[2.3 Asset owner / Line manager responsibilities 8](#_Toc142487135)

[2.4 User Responsibilities 9](#_Toc142487136)

[3 Enforcement 9](#_Toc142487137)

[4 References 9](#_Toc142487138)

# Introduction

## Purpose of this Document

The Access Control policy is defined in the LCETB ICT Framework Policy and should be read in conjunction with all other ICT policies to ensure that required security standards are adhered to. The purpose of this Access Control Policy document is to clearly specify how access to LCETB systems is managed and who may access information under what circumstances.

## Scope and Constraints

This policy is applicable to all Users of LCETB systems. The policy governs and applies to all user accounts created and managed by LCETB ICT Department or contracted 3rd party, on all systems, including test and development systems whether hosted locally or externally.

## Definitions

A full range of definitions is available in the ICT Frameworks Policy

## Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, who are committed to continually improving the protection of all LCETB information assets and the protection of personal data where LCETB is a controller or processor. This document will be reviewed at least every three years by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within LCETB.

# Policy

## ICT Responsibility / User account creation and management

* User and group permissions must be allocated based on the principles of least privilege.
* All user accounts must be assigned a unique identifier.
* Accounts should not be shared between users.
* All user logins across LCETB systems should be fully accountable and auditable, any system incapable of providing this feature must be noted on the risk register by the asset owner.
* Where possible authorisation should be granted based on group profiles (Role Based Access control), no unique permissions should be granted to an individual user account.
* All users should be issued with the ICT Acceptable Usage Policy prior to being given access to an account.
* A formally documented procedure (Such as a joiners/movers/leavers procedures) should define all access to LCETB technology infrastructure. The document should encapsulate the registration and de-registration procedure and should include:
	+ A check that the user has authorisation from the Asset Owner or delegated authority for use of the service (*e.g.* Line Manager)
	+ Verification of the requestor’s identity should be confirmed by means acceptable to [HR] prior to the request being processed.
	+ Where possible all access to LCETB information systems should be limited to a certain time span and with a defined expiry date.
	+ a check that the level of access granted is appropriate for the business purpose and is consistent with LCETB security and GDPR policies (including need-to-know and minimum rights principles).
	+ a check to ensure that redundant Login IDs are not reissued to another user unless controls are implemented to ensure that accountability is properly maintained.
	+ Confirmation that the account being requested is assigned to a specific individual user (should be no shared accounts, Basic “Tick box” confirmation).
	+ There must be a separation of duties such that the person who manages access is not the same person who authorises them (*i.e.* Asset Owners should not be control access).
	+ How to remove immediately all access rights from staff who leave LCETB.
	+ How to remove rights from staff who transfer within LCETB.
	+ Special attention is required when a member of the local IT Team with privileged rights is to leave or change roles. The de-registration procedures should include all steps required to remove such user rights.
	+ maintenance of an auditable formal record of accesses granted
* Login IDs should give no indication of the user’s level of authority (*e.g.* root, admin, manager, supervisor, auditor, monitor, *etc*.)
* An up-to-date list of the accounts on a system must be maintained or it must be possible to run a report on demand – this may be inside or outside the system but should contain an auditable record of the account authorisation, *i.e.* who signed off on the granting of access.
* The asset owner must ensure the following report is reviewed and actioned, privileges assigned to users must be revalidated annually. This review procedure must include:
	+ The list of all relevant user/group privileges to be reviewed.
	+ the review should confirm what action is to be taken, permitted, revoked,
	+ All redundant privileges must be removed and recorded as so.
* Retain auditable re-validation results, evidence of completion and supporting communications for at least two iterations.
* Where network or system access (*e.g.* NIST assessment) is required for use by a non-interactive system process (*e.g*. robotic application - no human interaction), this must be authorised by the relevant system owner and it should be connected to a host using a unique User ID and profile specifically provided for this use. Each such User ID has to have a specific owner.

## ICT Responsibilities / Logical Access Security Controls (including Security Hardening)

* All computer data which supports a LCETB business function must be protected by access controls to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable. At a minimum, access must be protected by passwords or similar approved authentication mechanisms, unless the access is explicitly intended for free public access (*e.g.* LCETB public internet site).

Specifically, anonymous access is not permitted to information systems, resources, data processing areas and communications networks of LCETB unless there is a business purpose to justify such access (public customer access to the company’s portal, *etc*.) or they have been specifically catalogued as public.

All hidden users, passwords, or other backdoors to the application should be removed. Examples of backdoors include (both malicious and due to programming errors):

* 1. Access to a specific URL of a web application in which the user has no access restrictions to all or certain data and functions.
	2. Unauthenticated connection to a system resource when initiated from a specific location or a specific user.
* All LCETB systems and third party services must have a documented build standard (hardening guide), that captures and maintains an industry-accepted system hardening configuration (Benchmark standard) that address all known vulnerabilities and system weaknesses, which can be audited for compliance when required. It is LCETB’s recommendation that the minimum of the Centre for Internet Security (CIS): http://www.cisecurity.org/; NIST http://web.nvd.nist.gov/view/ncp/repository; or equivalent should be used as the accepted system hardening security standard. Where CIS, NIST or SANS does not supply a security standard then an alternative appropriate industry or vendor standard should be identified and reviewed for appropriateness with the help and guidance of the LCETB ICT DEPT.
* All security recommendations listed within the approved security standards must be documented and separated into two distinct categories, security recommendations implemented and not implementable.
* All non-implementable recommendations should be reviewed every three years.
* All industry-accepted system hardening recommendations which cannot be implemented must be presented to the [ICT DEPT] documented business justification for non-compliance. Noncompliance must be recorded on the local risk register.
* Operating System and Platforms should be pre-hardened. Issues with a hardened OS should become apparent during the build and development stages of hardware deployment, rather than retrofitting security measures at a more mature stage of the process or project lifecycle.
* All operating systems, databases or other systems/application must conform to the documented standard. At a minimum, this must include:
	1. All non-essential programs or services must be shut down or disabled
	2. All security patches recommended by the vendor must be reviewed and installed
	3. Default systems accounts must be removed, locked, or have their name and password changed.
	4. Default access methods such as SNMP access with default community strings must be disabled or appropriately secured in line with password policy.
	5. LCETB Password Policy must be enforced on the system
* All System and Application Logins must display a legal banner prior to the authentication process. The purpose of a legal banner is to:
	1. Provide Legal Protection should evidence need to be collected from a device.
	2. Shield administrators from prosecution
	3. Acts as a deterrent to potential intruders.

This banner must be displayed prior to login, and must include:

 \*\*\* WARNING \*\*\*

This system is private and may be accessed only by authorised users for official purposes. The system owner reserves the right to monitor any and all activity taking place on this system and any attempts to connect to it. Individuals using this computer system are subject to having all of their activities monitored and recorded by system personnel. Use of this system evidences an express consent to such monitoring and agreement that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. Unauthorised users or users who exceed (or attempt to exceed), their authorised level of access are subject to prosecution under any local or international laws that apply as well as LCETB initiated proceedings. (Insert existing ETB banner, noting the guidance below, or use the above banner as required)

The legal banner must not contain:

* Any non-public information
* Mention of the purpose, location or owner of the device or any other identification information.
* It should not say “Welcome” anywhere in the description.

Where possible, the banner should be displayed on all interfaces to both the system and applications prior to authentication.

* A failure/rejection during the login sequence is not to indicate to the user which part of the login process failed. On completion of successful login, if the system supports the functionality, the following information must be displayed:
	1. date and time of previous successful login;
	2. A number of failed login attempts since the previous successful login.
* After a maximum of 10 consecutive failed authentication attempts, the account must be locked out to prevent brute-force password attempts. The account may be re-enabled by a third party with privilege access or automatically re-enabled after a period of time commensurate with the impact of Denial of Service (*e.g.* lockout an account for 24 hours after 10 consecutive failed login attempts).
* A time-out facility should clear the session screen and also, possibly later, close both application and network session after a defined period of inactivity (maximum of 30 minutes, however, the time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment). For example, all computer screensavers must be invoked after 30 minutes inactivity and the password must follow the LCETB password policy.
* System and Application Administrative interfaces should be restricted to authorised sources and not available to all of LCETB. This can be implemented on the firewall and/or on the systems themselves.
* It must not be possible to perform any type of system or application administration from the General Internet (even with a valid username/password).

## Asset owner / Line manager responsibilities

* Asset owners / Line Managers are responsible for ensuring that all physical and logical access is removed for personnel who are no longer working with LCETB or have transferred role within LCETB.
* Staff must not be assigned privileges that are likely to lead to a conflict of interest or security breach.
* When implementing access between separate third party systems, appropriate access levels must be determined and enforced. (*e.g.* MIS integration with Cloud Providers)

## User Responsibilities

* Users should not attempt to access data or systems to which they do not require access to complete their assigned work.
* Users should not share login credentials for any LCETB system with anyone.
* Users should not use the same combination of username and password for registering with external websites / systems for either work on personal use.
* User should report any potential breach or suspicious activity to the ICT DEPT Helpdesk.

# Enforcement

Individuals found to be in breach of this policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

# References

|  |  |  |
| --- | --- | --- |
| ISO27001 | NIST CSF | PCI-DSS |
|  |  |  |