

Access Management Policy



Version number	1.6
Last Approved	Mar 12, 2024
Classification	PUBLIC

Learning Technologies Group plc – Proprietary and Confidential – This document contains confidential information, which is the property of Learning Technologies Group plc, and may not be distributed externally without explicit written permission.

Overview

This Access Management policy describes provisioning, management, monitoring, and de-provisioning of user accounts and privileges, operating under the principle of least privilege.

Applicability

The applicability of this statement falls under purview of the [Security Documentation Overview](#).

Purpose

Access management controls are key to ensuring that the correct employees have access to the correct data and systems with the correct level. The Company's access controls are guided by the principle of least privilege and need-to-know to ensure security and privacy. The Access Management policy shall outline the Company's standard for user access and password management across all systems.

Scope

This policy applies to employee/contractor access to systems that process or store customer data

In the event of conflicting policy requirements governing the classification data processed and stored on Company owned IT Resources, Learning Technologies Group policies take precedence. If Personnel do not agree to abide by this Data Classification Policy, they should not be granted access to Company owned or controlled data. Any questions on this policy should be directed to the VP Information Security or to The Company's Legal department.

Access Management Policy

Principle of Least Privilege

Access controls must be allocated on the basis of business need and 'Least Privilege'. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

User Access Account Management

User account management procedures must be implemented for user registration, modification and de-registration on all Company systems.

These procedures must also include processes for monitoring redundant and inactive accounts. All additions, deletions, suspensions and modifications to user accesses should be captured in an audit log showing who took the action and when.

These procedures shall be implemented only by suitably trained and authorized employees.

Access control standards must be established for all information systems, at an appropriate level for each system, which minimizes information security risks yet allows the Company's business activities to be carried out without undue hindrance.

User access management reviews will be conducted quarterly for in-scope systems.

All access to Company information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity.

Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorized by the VP of Information Security or the VP of Hosting Systems and Operations.

All users shall have a user ID for their sole use for access to all computing services. All individual user IDs must be unique for each user and never duplicated.

Access to networks occurs through 2FA and VPN, controlled by various user access groups, inclusive of Active Directory and TACACS+.

All user accounts that have not been accessed for a period of inactivity appropriate for the systems, without prior arrangement, must be automatically disabled.

All administrator and privileged user accounts must be based upon job function and authorized by the Security team, prior to access being given. All changes to privileged accounts must be logged and regularly reviewed.

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organization.

Users' access rights will be reviewed at quarterly. Access to systems by individual users must be authorized by their manager or where applicable, the VP of Information Security.

Password Management

Passwords must not be shared with any other person for any reason. All default system and vendor passwords must be changed immediately following installation.

All Company information systems must support strong password management techniques (such as: length, complexity, aging, history, account lockout).

Users shall only use approved password managers to store company related passwords and credentials, including encryption keys and pass-phrases.

Users shall use secure password tools like [One Time Secret Password](#) when applicable.

All Company information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter on a regular basis. Review CITO's [Password Policy](#) for further information on password criteria and guidelines.

Monitoring User Access

Systems will be capable of logging sufficient events that have a relevance to potential breaches of security. User access will be subject to management checks. Programs with the ability to override system controls will be closely monitored.

Responsibilities

VP of Information Security

The VP of Information Security is responsible for ensuring that the requirements of this policy are implemented within any program, projects, systems or services for which they are responsible.

The VP of Information Security is responsible for ensuring that a robust checking regime is in place and complied with to ensure that legitimate user access is not abused.

The VP of Information Security may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regime.

Any non-compliance with this policy must be supported by a documented and evidence based risk decision accepted by the VP of Information Security.

Managers

Managers are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job and comply with role-based access principles.

Managers should ensure that the access rights of people who have a change of duties or job roles or left the organization are revoked promptly.

All Managers should review the access levels of their people to ensure they are appropriate.

Security and Hosting Teams

Security and Hosting Teams are responsible for granting access to systems as described in local work instructions or use of Role Based Access Controls Matrix in accordance with the relevant procedures.

Security and Hosting Teams must evaluate and, if necessary, challenge authorized access to help identify any obvious anomalies in the access levels granted or requested.


Users

Users must only access Company systems and data for legitimate use as required by their job and role.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the [Security Documentation Overview](#) .

Document control

 This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado
Author(s)	@Art Machado @Sarah Zwicker (Unlicensed) @John Cole

Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 12, 2024
Review cycle	ANNUAL	
Next review date	Mar 12, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 01, 2024	@angelina.kilmer	1.6	Updated Policy classification from Confidential to Public
Mar 12, 2024	@Art Machado , @Sarah Zwicker (Unlicensed) @Paul Gordon	1.5	Annual review
Dec 4, 2023	@Sarah Zwicker (Unlicensed)	1.4	Linked Password Policy
Aug 29, 2023	@Sarah Zwicker (Unlicensed)	1.3	Removed ISO Annex control language
Feb 23, 2023	@Art Machado , @Sarah Zwicker (Unlicensed)	1.2	Annual review + logo updated
Apr 13, 2022	@Sarah Zwicker (Unlicensed)	1.1	Initial Review and Approval
Mar 31, 2022	@Art Machado , @Sarah Zwicker (Unlicensed)	1.0	Original version