

Global Information Security Training for Contractors Policy



Version number	1.2
Last Approved	Nov 1, 2023
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

Information stands as one of LTG's vital business resources alongside its people and products, demanding careful protection. Clients, customers, partners, licensors, and suppliers entrust LTG with confidential information crucial to their businesses. Disclosure of such information could significantly impact LTG's relationships, standing in the technology community, and even its competitive advantage. Therefore, all confidential, classified, and proprietary information under LTG's control ("Confidential Information") must be appropriately safeguarded.

Applicability

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

Purpose

The policy's primary aim is to ensure that all contractors working with LTG complete mandatory Information Security Training. It's imperative that contractors adhere to the same information security standards as employees to safeguard the company's sensitive data and information.

All contractors engaged by LTG must read, understand, and comply with this policy. Full cooperation is expected from contractors to maintain the integrity and confidentiality of LTG's data and systems.

For a detailed understanding of LTG's approach and responsibilities regarding confidential information, refer to the Confidential Information Policy located [here](#).

Scope

This policy applies to all external contractors engaged by LTG who have access to the company's information systems, data, or physical premises.

Global Information Security Training for Contractors Policy

Contractor onboarding

1. Before commencing work with LTG, all contractors must successfully complete the mandatory Information Security Training, covering relevant policies, procedures, and best practices for safeguarding company information.

Contractor information handling

2. Contractors must comply with all information handling policies, including data classification, storage, transmission, and disposal practices. Any sensitive or confidential data accessed during their contractual work must be treated with the utmost confidentiality and protected in accordance with company policies.

Contractor access control

3. Contractors will be provided with necessary access strictly limited to the requirements of their role. Sharing access credentials or allowing unauthorised access to company systems is strictly prohibited.

Contractor security awareness

4. Contractors are expected to remain vigilant and report any suspicious activities, security breaches, or vulnerabilities immediately to the designated point of contact within the company. Regular refresher courses and awareness programs will keep them updated on security practices.

Contractor status

5. Completion of any LTG training does not infer employment status with the Company. It's solely the Company's execution of its information security obligations.

Consequences of non compliance

6. Unsuccessful completion or refusal of Information Security Training may be considered a serious breach, leading to immediate termination of the contractor agreement.
7. Failure to adhere to this policy or breach of information security standards may result in termination of the contract and necessary legal actions by the company.

Policy compliance

8. The Information Security Department is responsible for monitoring and ensuring compliance with this policy. Regular assessments, audits, and checks will confirm contractors' adherence to established information security practices.

More information

9. Please reach out to the IT Team via the [IT Helpdesk](#) should you need more information.

Document control

i 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	@Stefan Larsen		
Author(s)	@Stefan Larsen , @Heather Wood		
Required Approver(s) and Approval Date	@Heather Wood - HR Director		Nov 1, 2023
	@Stefan Larsen - People Ops Director		Nov 1, 2023
Review cycle	ANNUAL		
Next review date	Nov 1, 2024		

Version History

Date	Author(s)	Version	Changes
Nov 1, 2024	@angelina.kilmer	1.2	Changed Policy classification from Confidential to Public
Nov 9, 2023	@Sarah Zwicker (Unlicensed)	1.1	Published on Confluence
Nov 1, 2023	@Stefan Larsen	1.0	Original