

Security Documentation Overview



Version number	2.5
Last Approved	Mar 13, 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.

Applicability

The Company's solutions are delivered in a Software-as-a-Service ('SaaS') model, collectively referred to as the SaaS Offerings. These policies apply to the following business units:

- Affinity
- Breezy
- Bridge
- OpenLMS
- PeopleFluent
- Preloaded
- Rustici Software
- Watershed Systems
- VectorVMS

Systems shall be governed by Security policies outlined as part of the this Overview. Hosting systems may require varying or more rigorous security requirements, which may necessitate prevailing Hosting-specific policies.

These policies apply to LTG Central Services (HR, IT, Finance, Legal, Facilities) to the extent applicable due to dependencies.

Overview

The Security Documentation Overview is a broad synopsis of The Company's Information Security and Privacy policies. It outlines each policy's contents as well as containing overarching statements on Applicability, Continuity, and Oversight.

Purpose

The objective of the Security Documentation Overview is to provide a comprehensive index and provide policy control guidelines. This document provides the scope, controls structure and measures, and acts as governing statements for documents in the ISMS family.

This overview will act as a "**Master Table of Contents**", outlining all Company Security and Privacy policies, as well as documenting versioning, ownership, and ISMS Management approval dates. Each policy will be reviewed at least annually, with its version and changes noted by the author in that policy's Change log.

▼ ISO 27001:2013 Control 7.5.2

When creating and updating documented information the organization shall ensure appropriate:

- a) identification and description (e.g. a title, date, author, or reference number);*
- b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and*
- c) review and approval for suitability and adequacy.*

▼ ISO 27001:2013 Control 7.5.3

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

- a) it is available and suitable for use, where and when it is needed; and*
- b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).*

For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

Scope

The policies included in this Security Documentation Overview apply to the business units providing SaaS offerings for our customers and the data processed therein. These policies apply to all employees, including contractors.

Where applicable, and when a third party provides some or all of a hosted product's infrastructure, The Company shall ensure that the third party's security commitments are at least as rigorous as The Company's.

Master Table of Contents

[Acceptable Use Policy \(AUP\)](#)

The Acceptable Use Policy (AUP) stipulates constraints and practices that Company Personnel must abide by while accessing and using The Company's resources and data, or client data. This policy covers areas which include but are not limited to: hardware, software, email and messaging, data storage, PII, internet, wireless networking, blogging, social media, and third party services.

[Access Management Policy](#)

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

[Bring Your Own Device \(BYOD\) Policy](#)

The Bring Your Own Device (BYOD) Policy defines who can access Company systems using non-Company issued devices, their responsibilities in doing so, and Company's monitoring and access to the device.

[Business Continuity and Risk Management Policy](#)

The Business Continuity and Risk Management defines the process in which The Company performs Business Impact Analysis to develop a risk-based resiliency plan.

Disaster Recovery (DR) addresses customer-facing continuity in its hosted systems and is inclusive of customer data.

The policy ensures that The Company will perform regularly scheduled risk assessments and BCP / DR testing to align The Company's capabilities with its risk posture.

[Client Data Privacy Compliance Policy](#)

The Data Privacy Compliance Policy provides the framework for The Company's requirements for implementing and maintaining privacy compliance across all applicable laws and regulations.

Data Backup Policy

The Data Backup Policy provides minimal guidance on the retention, duration and the backup and restoration methodologies used to securely store copies of systems in a manner that protects the privacy of data and the integrity of copies of the SaaS hosting infrastructure and client data. These guidelines meet industry best practices and ensures The Company retains 'safe' immutable backup copies to prevent data loss due to physical destruction or retroactive modification. The disposition of backup media is covered by the [Data Retention, Destruction and Disposal Policy](#).

Data Classification Policy

The Data Classification Policy defines the levels of data classification and the types of information that fall into each category. This policy also defines the appropriate level of security and access controls for each classification.

Data Retention, Destruction and Disposal Policy

The Data Retention, Destruction and Disposal Policy defines how long The Company retains data and how it sanitizes, deletes, and disposes of client data and physical hardware used in the hosting of customer data. The policy specifies requirements for data retention, secure destruction and documentation to meet industry best practices and ensure security and privacy for customer data. An overview of how data is backed up is covered by the [Data Backup Policy](#).

Encryption Key Management Policy

The Encryption Key Management policy defines the requirements used to control public and private encryption keys and defines their lifecycle, inclusive of creation, usage, storage, and deletion.

Information Security Statement

The Information Security Statement provides a framework that will ensure the protection of The Company's assets and its customers' data and privacy. The statement outlines the Information Security Mission and Strategy, as well as the security roles and responsibilities.

Internal Audit and Compliance Policy

The Internal Audit and Compliance Policy establishes the use of audits and/or other evaluation techniques to ensure effective oversight of controls performance and hosting activity.

The Company shall establish a process to ensure that our operations and products are in compliance with applicable laws, regulations, policies, procedures, and the [Code of Conduct](#).

Inventory and Ownership of Assets Policy

The Inventory and Ownership of Assets Policy defines responsibilities for company assets at all levels of the business. Roles are defined and the global inventory system is explained.

Non-Client Data Retention Policy

The Non-Client Data Retention Policy outlines The Company's standards regarding the data retention of non-client data only.

Password Policy

The Password Policy's purpose is to outline The Company's standards for using passwords so that devices, software and services are appropriately protected to ensure privacy and protection of Company and customer data.

Physical Security Policy

The Physical Security Policy defines The Company's security controls for facilities and aligns these controls to the principle of least access for all persons visiting our locations. The policy also defines tracking and documentation requirements for all facility access.

Security Baselines Policy

The purpose of this document is to provide guidance on how IT systems should be configured. What software versions are allowed on the LTG network to maximize the protection of the confidentiality, integrity and availability of data processed. Besides the requirement the system to be designed with security in mind right from the scratch, the subsequent related actions often involve (but are not limited to) the following:

- Configuration hardening.
- Presence of means for privilege separation.
- Periodically updating the underlying system software with latest patches
- Presence of system tools regularly performing security scans, integrity checks, backups etc.

Security Event/Incident Response Plan

Security events present a threat to the confidentiality, integrity, and availability of The Company's systems and data. Successful mitigation of this threat requires not only a best practice approach to managing system vulnerabilities, but also swift and effective response to any security events.

The procedures defined in this document ensure that security events affecting The Company are appropriately and consistently identified and handled.

Secure Software Development (SDLC) Policy

The Secure Software Development Policy provides a documented description of how software is built and maintained, emphasizing privacy and security. It describes the various phases of the development process and activities performed during each phase.

Vendor Management Policy

The Vendor Management Policy establishes criteria for adoption and qualification of new vendors, evaluation of vendor performance and compliance, risk identification and mitigation, and termination of a vendor relationship.

Vulnerability Management Policy

The Vulnerability Management Policy defines the types of activities for regular vulnerability assessment of hosted / customer-facing systems. Internal vulnerability assessment activities and the time frames for each are defined, as is the use of independent parties for validation and verification. The policy addresses patching requirements for third party components and requirements governing customer testing.

This policy defines our methodology and remediation time frames for any findings.

Additional Information - Continuity and Oversight

The following statements on *Oversight*, *Disciplinary Actions*, *Exceptions*, and *Questions* contained within this policy are applicable and enforced throughout the above listed policies, statements, and measures.

Executive Security Steering Committee Oversight

Changes to these policies will be communicated to the Executive Security Steering Committee as necessary.

Executive Security Steering Committee will be established and will include executives and technical representatives for each applicable group within The Company.

Disciplinary Actions

Violation of the above policies may result in disciplinary action which may include termination of employment, dismissal, or suspension. Additionally, employees, contractors, and agents who violate this policy may be subject to civil and criminal prosecution.

Exceptions

The Company's Information Security Policies (and the procedures developed and approved to implement them) should be applicable in most circumstances. However, The Company recognizes that some circumstances require deviations from standard policies and procedures. Exceptions must be rare and must be based on sound rationale. An exception register will be maintained by the VP of Information Security and will be reviewed at least annually.


Recent Acquisitions

Products or companies acquired within the last 6 months that otherwise would be in scope must develop a transitional plan and may continue to operate under their prior information security policies so long as they do not conflict with the spirit of these documents. The acquired product(s) must transition to this plan, either by adoption as it stands or by proposing changes to this policy that meet the spirit and intent and will not jeopardize compliance of other product lines. After a period of six months, any acquired products or companies will fall within the scope of the most recent revision of this policy.

Questions

Any questions about this document should be directed to the [Security Team](#).

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)		
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 13, 2024	
Review cycle	ANNUAL		
Next review date	Mar 13, 2025		

Version History

Date	Author(s)	Version	Changes
------	-----------	---------	---------

Nov 1, 2024	@angelina.kilmer	2.5	Changed Policy classification from Confidential to Public
May 9, 2024	@Sarah Zwicker (Unlicensed) @Art Machado	2.4	Added LTG Central Services to Applicability statement
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	2.3	Annual review; update Company legal entity and scoping considerations; inclusion of IT policies
Mar 11, 2024	@Sarah Zwicker (Unlicensed)	2.2	Updated Disciplinary Action language
Jan 16, 2024	@Sarah Zwicker (Unlicensed)	2.1	Moved to Global Policy Register, updated applicability statement
Apr 14, 2023	@Sarah Zwicker (Unlicensed) @Art Machado	2.0	Applicability statement clarifications
Feb 23, 2023	@Sarah Zwicker (Unlicensed)	1.9	Annual review + logo change
Nov 15, 2022	@Sarah Zwicker (Unlicensed)	1.8	Added "Bridge Advance Video" to Instilled's name
Apr 22, 2022	@Sarah Zwicker (Unlicensed)	1.7	Additions of PF-ISMS-0019, PF-ISMS-0020, PF-ISMS-0021; Added Privacy considerations
Mar 16, 2022	@Sarah Zwicker (Unlicensed) @Art Machado	1.6	Annual Review; Changes to Applicability to reflect acquisitions; Title change for VP InfoSec
Nov 18, 2021	@Sarah Zwicker (Unlicensed)	1.5	Changed name of PF-ISMS-0008 after policy was modified to include Data Retention
Nov 12, 2021	@Sarah Zwicker (Unlicensed)	1.4	Added PF-ISMS-0018
Jul 28, 2021	@Sarah Zwicker (Unlicensed)	1.3	Updated Policy Titles
Apr 9, 2021	@Sarah Zwicker (Unlicensed)	1.2	Inclusion of applicable ISO controls
Mar 15, 2021	@Sarah Zwicker (Unlicensed)	1.1	Changed owner Changed ISMS Required Approvers and Dates Deprecation of PF-ISMS-0012, and is now addressed within PF-ISMS-0009 Deprecation of PF-ISMS-0015, and is now included within PF-HOST-0015

Feb 2, 2021	@Sarah Zwicker (Unlicensed) @Art Machado	1.0	Original version
-------------	--	-----	------------------