

Vendor Management Policy



Version number	3.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

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

Overview

This 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.

Applicability

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

Purpose

This policy ensures The Company has performs its due diligence in regards to assessing vendor risk and performance to ensure the security and privacy of Company and customer data.


Scope

This policy applies to vendors providing services within the scope of The Company's development and hosting of client-facing systems, or any vendors that may contain employee or client PII.

Vendor Management Policy

Prerequisites

1. Vendor classification: a system-generated vendor list must contain **all** vendors within scope, each classified in accordance with **risk** or **impact** to The Company's services
2. SOC 2 reports must be requested in advance for vendors classified as high-risk or sub-processors. If the vendor is not SOC 2 accredited, supplemental documentation may be acceptable (security questionnaire, security page, penetration test report, risk assessment reports, etc.).

 Raise a ticket [here](#) for the GRC team to evaluate your prospective vendor

New Vendor Due Diligence

Prior to onboarding new vendors, The Company must perform due diligence to ensure that engaging the vendor does not pose unreasonable risk to The Company or its customers. Vendors must be held accountable to the same level of commitments The Company makes to its customers. Findings against a vendor are listed in the Vendor Risk Log and any of a Critical or High risk level are recorded in the Company's Risk Register.

✓ SOC 2: CC9.2

The entity assesses and manages risks associated with vendors and business partners.

Depending on the service provided, vendors can be classified according to their risk level:

Critical Risk/Sub-processors

Criteria

- Vendors that have access to, store, or process personally identifiable information (PII), confidential or restricted information, or production data.
- ALL sub-processors are Critical risk vendors.
- Vendors that pose the highest risk if data is lost, including breach of contract or regulatory compliance risk.
- Vendors who's downtime could result in failure or inability to deliver services.
- Vendors that pose a high financial risk and may be difficult to replace.
- Critical vendors are embedded into core networks, applications, or processes

Process

- Critical risk vendors are considered the highest risk vendors and therefore, undergo a thorough review when onboarding and annually.
- Applicable SOC reports and Certifications need to be reviewed and verified.
 - Review SOC 1 Type 1 for Financial Tools and PCI compliance for payment processors. SOC 2 Type 2 for all others.
 - Supplemental documentation may be acceptable (ISO Certification, HIPAA compliance, security questionnaire, security page, penetration test report, risk assessment reports, etc.).
 - Review entails mapping specific Company Controls to recommended Complementary User Entity Controls (CUECs).
 - Exceptions in compliance reports are reviewed for potential risk to The Company.
- Any recent security breaches and lawsuits are notated and reviewed.
- Acceptable Data Processing Addendum and/or Security Addendum is obtained.

High Risk

Criteria

- Vendors that touch confidential, restricted, or internal data. This includes business operations or private data.
- Vendors whom the Company is highly dependent on operationally and make require some effort to replace, but not Critical.
- Vendors who's downtime could result in disruption with significant impact on the Company's service but not at the level of Critical risk vendors.
- Vendors that pose a medium financial risk and may be hard to replace.
- High risk vendors support core functions and may include some APIs.

Process

- High risk vendors undergo a detailed review when onboarding and annually.
- A streamlined review of any applicable SOC reports, industry certifications are reviewed and verified including CUEC mapping and review of potential risks found in compliance report exceptions.

Medium Risk

Criteria

- Vendors that touch internal data that supports supplemental services.
- Vendors who's loss of service does not cause significant disruption.
- Medium risk vendors are typically low cost and easily replaceable.
- Medium risk vendors may have access and visibility into processes but not directly integrated, if only by APIs.

Process

- Review of medium risk vendors entails an inspection of security controls as stated on security pages, whitepapers, or policies.
- Review of medium risk vendors does not require review of CUECs.

Low Risk

Criteria

- Vendors that touch public data.
- Vendors who's loss of service has no impact on Service Level Agreements.
- Low risk vendors are low cost and easily replaceable.
- Low risk vendors have no integration into our environments or products.

Process

- Low risk vendors pose little to no impact on the Company's service and therefore, do not require review prior to onboarding or annually.

Vendor Risk Rating Matrix

	Critical	High	Medium	Low
Who is the Data Controller	Client LTG	Client LTG	LTG	LTG
Is the Vendor a Sub-Processor?	Yes	No	No	No
Data Type	Confidential & Restricted	Confidential & Restricted Internal	Internal	Public
Risk if data is lost	Breach of contract Regulatory compliance risk	Highly dependent on service operationally and may require some effort to replace, but not Critical	Loss of data may be disruptive	No impact on SLAs
Access to data	Accesses customer and/or employee PII or proprietary data Read/write access	Access to business operations or private data	Supports supplemental services	Public data None

Downtime impact? / Disruption of service? If this fails, will it impact client SLAs?	Failure or inability to deliver could result in organisational failure/SLA failure	Disruption with significant impact on service but not at the level of service failure	Loss of service may be disruptive	No impact on SLAs
Financial Risk (how much are we paying for the service)	High Cost	Medium Cost May be hard to replace Niche services	Low cost Easily replaceable	Low cost Easily replaceable
Essential function/service?	Yes, embedded into our networks, apps, or processes	Supports core functions	Access and visibility into processes but not be directly integrated	No integration to our environments or products

New vendors are assessed based on information provided in the [Vendor Assessment Form](#) and undergo due diligence depending on the assessed level.

Due diligence can be performed in a number of ways.

1. For vendors with a **compliance certification** or **accreditation**, the compliance report can be obtained and reviewed to ensure that the vendor's control environment is sufficiently designed and operated to maintain The Company's commitments to customers. The same procedure for performing an annual vendor review, detailed in the following section, can be performed when reviewing compliance reports.
2. If the vendor does not have any compliance report available, due diligence can be accomplished by reviewing **alternate documentation regarding the vendor's controls**, such as a security page on their website, penetration test report, vulnerability assessment report, or a security questionnaire.

Vendor contracts must be reviewed to verify that the vendor can maintain the confidentiality commitments made to The Company's clients. If provisions for confidentiality are not explicitly stated in the contract, alternate documents may be reviewed for similar assurance, such as standard terms of service or end user agreements.

Critical or high risk vendors can only be onboarded once the due diligence has been completed, documented and approved by the VP Information Security.


Review Cadence

All vendors must be reviewed prior to onboarding, and annually reviewed as risk, security and compliance are dynamic and constantly evolving. Vendors onboarded less than 9 months from the annual review are exempt from reevaluation.

Offboarding Vendors

Due diligence and risk management must be performed throughout the vendor lifecycle, including when offboarding a vendor. Below are two key considerations to consider whenever a vendor is being offboarded.

Data Deletion

When terminating a relationship with a critical risk vendor, The Company must ensure that the vendor deletes all confidential data retained from the lifetime of the engagement within a reasonable timeframe. Deletion of confidential data stored by the vendor not only protects The Company's sensitive information but also helps achieve The Company's confidentiality commitments to its own customers. Refer to [a Retention, Destruction and Disposal Policy](#)  for compliance guidelines.

Preservation of Audit Evidence

Record of prior vendor assessments must be maintained for a period of 5 years. Evidence of offboarding and data deletion, as applicable, must be maintained for that period.

Additional Information

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

Supporting Procedures

[Vendor Management Procedure](#)

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	@Art Machado		
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon		
Required Approver(s) and Approval Date	@Art Machado - VP Information Security		Feb 25, 2025
Review cycle	ANNUAL		
Next review date	Feb 24, 2025		

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@Art Machado @angelina.kilmer @Paul Gordon	3.0	Annual review
Nov 1, 2024	@angelina.kilmer	2.2	Changed Policy classification from Confidential to Public
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	2.1	Annual review
Oct 26, 2023	@angelina.kilmer & @Sarah Zwicker (Unlicensed)	2.0	Updated Vendor Risk criteria/process as it relates to due dilligence

Sep 21, 2023	@Sarah Zwicker (Unlicensed) & @John Cole	1.7	Format updated, moved to Global Policy Register
Aug 3, 2023	@Sarah Zwicker (Unlicensed) & @John Cole	1.6	Updated scope to include employee PII, revised offboarding and added link to procedure.
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	1.5	Annual review + logo change
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	1.4	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	1.3	Title change for VP InfoSec, Annual Review
May 25, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	1.2	Pulled out procedure elements and created new Vendor Management Procedure .
Mar 11, 2021	@Sarah Zwicker (Unlicensed)	1.1	Changed formatting, added Document Control, Change log, confidentiality statement and added references to LTG.
Feb 24, 2021	@Art Machado	1.0	Original version