

Vulnerability Management Policy



Version number	4.0
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 [↗](#)

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.

Applicability [↗](#)

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

Purpose [↗](#)

To ensure that The Company consistently identifies and remediates vulnerabilities and its application solutions and infrastructure promptly and in a way that aligns with customer expectations and industry standards to ensure security and privacy.

Scope [↗](#)

This document covers vulnerability management for all Company developed and/or hosted application solutions and infrastructure.

Vulnerability Management Policy [↗](#)

Vulnerability Classifications [↗](#)

All vulnerabilities are subject to the same classification system and remediation SLAs.

Severity	Remediation SLA
Critical	ASAP (not to exceed 30 days)
High	30 days
Medium	90 days

Low

Prioritized backlog

Vulnerability Testing & Proactive Detection [↗](#)

The Company shall proactively attempt to detect vulnerabilities in their software products. This shall be done by performing regular vulnerability tests against both engineering releases and SaaS deployment environments.

✓ SOC 2: CC6.8, CC7.1

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Network Scanning [↗](#)

External Vulnerability Scanning [↗](#)

Definition: a network port scan initiated from a system outside our controlled network, which mimics the access that a potential bad actor could have to our systems.

The Company's Hosting Services team will perform external vulnerability scanning for each Company-hosted product line on a monthly basis.

Internal Vulnerability Scanning [↗](#)

Definition: a network port scan initiated from a system trusted by our controlled network, which could potentially have more access than a potential bad actor could have to our systems.

The Company's Hosting Services team will supplement internal vulnerability scanning with internal scans on an as needed basis to ensure comprehensive vulnerability testing coverage.

Internal Network/Application Penetration Test [↗](#)

Definition: an internal network/application penetration tests utilizes port scan as well as tools that are designed to manipulate data or APIs to or from a system conducted by Hosting Services.

The Company's Hosting Services team will supplement other types of internal penetration testing with internal scans on an as needed basis to ensure comprehensive vulnerability testing coverage.

Infrastructure Patching [↗](#)

The Company's Hosting Services team is responsible for monitoring and patching vulnerabilities in 3rd party infrastructure and Hosting Services software.

Client-Initiated Vulnerability Scanning [↗](#)

Upon request, clients may be authorized to perform their own external vulnerability scans of The Company's Hosted Solutions; this must be requested and approved on a case-by-case basis by both Hosting and Security management.

Client-initiated vulnerability scans follow these guidelines:

- tests must be limited to non-production environments;
- testing must only occur during pre-approved timeframes;
- testing may not include DDoS or other load-based testing techniques;
- client emergency contact must be identified who can immediately address any disruption caused by the testing.

Application Vulnerability Testing [↗](#)

Static Application Security Testing (SAST) [↗](#)

Each of The Company's product engineering teams must perform Static Application Security Testing as a required step its software development life cycle. Each team may use its own discretion in determining the timing and cadence for this testing as long as it is performed for **all** new major release candidates.

Dynamic Application Security Testing (DAST) [↗](#)

Each of The Company's product engineering teams must perform Dynamic Application Security Testing as a required step its software development life cycle. Each team may use its own discretion in determining the timing and cadence for this testing as long as it is performed for **all** new major release candidates.

Dynamic Scanning should only be performed in Engineering verification and validation environments.

Software Composition Analysis (SCA) [↗](#)

Software Composition Analysis is used to identify vulnerabilities in 3rd party code that is being used in Company applications.

Each of The Company's product engineering teams must perform Software Composition Analysis as a required step its software development life cycle. Each team may use its own discretion in determining the timing and cadence for this testing as long as it is performed for **all** new major release candidates.

Software License Management [↗](#)

The objective of Software License Management is to ensure that The Company is tracking the licensing which applies to all 3rd party software that it is leveraging within its application solutions and to identify any applicable licensing which presents potentially problematic terms and conditions.

Each of The Company's product engineering teams is responsible for tracking the licenses for any 3rd party software components that it is using within the product line. This information must be readily accessible and up to date for periodic assessment.

External Application Penetration Testing [↗](#)

The Company will engage an accredited 3rd party service provider to perform penetration testing on all its active product lines, as deemed necessary, on at least an annual basis. The scope of penetration tests must follow industry best practice. As with all vulnerability testing, these penetration tests must be performed in non-production hosted environments, which replicate production sites.

Vulnerability Management Life Cycle [↗](#)

All production systems must have protections in place to prevent the spreading of viruses and malware. This must be accomplished using a combination of file scanning and zero day mitigation.

Vulnerability Triage [↗](#)

Results of vulnerability testing must be promptly assessed to validate each finding and to verify appropriate severity classification. The hosting and engineering teams performing the testing are responsible for this initial triage and subsequent assignment and scheduling of remediation work as appropriate. Triage results are subject to Security Team review and approval. Vulnerability classifications are based on industry standards and any adjustments to classifications must be approved by The Company's Security Team.

In the case of client-initiated vulnerability scans or 3rd party penetration tests, The Company's Security Team is responsible for triage in collaboration with the appropriate internal teams.

Vulnerability Remediation [↗](#)

Vulnerability test findings, once triaged and assigned, must generally be remediated within the prescribed timelines associated with each severity classification (see Remediation SLA table above). Exact remediation timelines for non-critical vulnerabilities may be adjusted to align with relevant release schedules. However, any significant variances from the standard remediation timeline must be approved and managed by the Security Team.

SaaS Environment Monitoring

The Company shall actively monitor system components and operational configurations to prevent the introduction of new vulnerabilities resulting from configuration or operational deployment choices.

The monitoring methodology may vary due to deployment choices, but likely includes one or more of the following type of applications: real-time security monitoring platforms (SIEM systems), AV or Malware agents, WAFs, and zero-day prevention systems.

Anti virus/malware scanning is required:

1. For all client uploads
2. At build time for all containerized environments
3. For all non-containerized/non-read-only environments

Anti virus/malware scanning may be performed via periodic full scans or minimally upon file access.

✓ SOC 2: CC7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Confidentiality of Vulnerability Management Data


Vulnerability testing techniques, tools, and results are all considered highly sensitive and confidential internal information and may not be shared externally under any circumstances. A summary of any vulnerability test may be provided by the Security Team upon request and requires an NDA.

Disclosure of vulnerability details is permissible in the context of a Security Incident as defined in the Security Incident Response Plan.

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	@Paul Gordon	@angelina.kilmer
Required Approver(s) and Approval Date	@Art Machado - VP Information Security		Feb 25, 2025
Review cycle	ANNUAL		
Next review date	Feb 24, 2026		

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@Art Machado @angelina.kilmer @Paul Gordon	4.0	Annual review
Oct 28, 2024	@Art Machado @Paul Gordon @angelina.kilmer	3.2	Malware scanning updates. Changed Policy classification from Confidential to Public
Mar 28, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	3.1	Annual review
Jul 25, 2023	@John Cole	3.0	Updated monitoring and prevention methods
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.9	Annual review + logo updated
Nov 30, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.8	Added section on scanning + zero day mitigation
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.7	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.6	Title change for VP InfoSec, Annual Policy Review
May 18, 2021	@Art Machado	2.5	Policy re-written to match updated Company standards.
Mar 11, 2021	@Sarah Zwicker (Unlicensed)	2.4	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.3	Reformatted, policies linked
Jan 26, 2021	@John Cole	2.2	Annual review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.1	Changed owner. Added sections to refer to LTG policies and organizational change.