Proficiencee

Security Overview

Last Updated: July 2026

Proficiencee consists of a Canvas-based learning management platform and Proficiencee LTI learning tools (assessments and guided learning) that launch from an LMS via LTI. This document describes security for the Proficiencee platform overall; where Canvas LMS and LTI tools differ, both are noted.

Table of Contents

Type of Sensitive Data Proficiencee Manages

Regulated Data

Category	Applies?
PCI regulated (credit card data)	No
FERPA regulated (student data)	**Yes**
HIPAA regulated (health data)	**Yes**
ITAR (import, export, defense-related technical data or foreign students)	No

HIPAA: Proficiencee LTI tools may collect health-related assessment responses used in educational wellness programs. Where HIPAA applies to an institution's use of the platform, obligations are addressed through appropriate contractual arrangements (for example a Business Associate Agreement) as required.

Data Classifications

Category	Applies?
Highly Sensitive — disclosure endangers human life, health, or safety	No
Sensitive — regulated data (including regulations above) or Personally Identifiable Information	**Yes**
Internal — a login is required	No
Public — anyone can see it without logging in	No

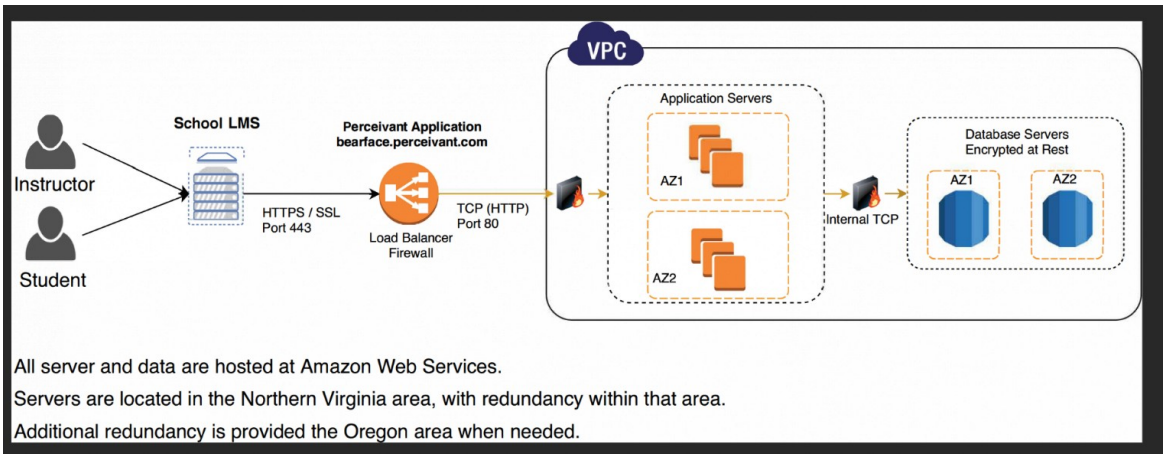
Data Protection During Travel Across Networks

All web sites are using https encryption. Servers have valid https certificates. The certificates are correctly configured and installed so that no warnings are seen. All sensitive data is encrypted as it travels over each network connection.

Data Protection at REST (Storage)

Sensitive data is encrypted at rest using AWS-managed encryption for databases, volumes, object storage (S3), and backups as configured in the Proficiencee production environment. Employee workstations that may access production systems are required to use full-disk encryption and password protection per internal policy.

Security Architecture Diagram



Security Infrastructure

The Proficiencee education technology platform is hosted on cloud infrastructure provided by Amazon Web Services (AWS). The AWS infrastructure is highly stable, fault-tolerant, and secure as attested by AWS certifications and attestations (including SOC 2 Type II and ISO/IEC 27001 — current edition — and PCI DSS as a Level 1 service provider for AWS). These are AWS provider certifications; they do not by themselves mean Proficiencee processes cardholder data.

For additional information about AWS security certifications and standards compliance, please refer to the following:

- https://aws.amazon.com/security
- https://aws.amazon.com/compliance

AWS Network Security

The AWS cloud infrastructure provides extensive network and security monitoring systems to protect the Proficiencee production environment and its data. These systems protect against:

- **Man In the Middle (MITM) Attacks.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon Elastic Compute Cloud (EC2) Amazon Machine Images (AMIs) automatically generate new Secure Shell (SSH) host certificates on first boot and log them to the instance's console.

- **IP Spoofing.** Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning.** When port scanning is detected, it is stopped and blocked.
- **Virtual Private Cloud.** Proficiencee utilizes VPCs in order to further segment, protect, and isolate Proficiencee network traffic.

AWS Services

The AWS services used to host Proficiencee include Elastic Compute Cloud (EC2) and/or Elastic Container Service (ECS/Fargate), Elastic Load Balancing (ELB), Auto Scaling, Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC), Identity and Access Management (IAM), and related supporting services (for example email and caching as configured). The Proficiencee application is designed to use AWS redundancy and capacity capabilities, running across multiple availability zones. Primary object storage is provided by Amazon S3.

AWS Regions and Data Centers

Amazon EC2/ECS is hosted in multiple locations worldwide comprising regions and Availability Zones. Proficiencee production workloads for U.S. client institutions are hosted in U.S. AWS regions — primarily US East (Northern Virginia), with redundancy in US West (Oregon). AWS data centers utilize electronic surveillance and multi-factor access control; environmental and power systems are designed for high availability.

AWS data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least-privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones provide resilience in the face of most failure modes including natural disasters or system failures.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Generators provide backup power for the data centers of the entire facility.

AWS Data Security

All data traffic in and out of Proficiencee is encrypted using TLS, forward-secrecy-compliant ciphers whenever possible (e.g. ECDHE-ECDSA-AES128-GCM-SHA256). The acceptable cipher list is constantly maintained to ensure that no vulnerabilities are present (e.g. POODLE). Data is stored redundantly in multiple data centers and multiple geographic regions through Amazon S3. The Proficiencee architecture replicates data in near real-time and data is backed up on a daily basis. Proficiencee creates daily offsite database backups of Proficiencee data and content including course structures, coursework, analytics, rubrics, learning outcomes, and metadata. Proficiencee data replication and backups ensure that, in the event of a necessary system restore, the potential data loss would be limited.

Web Site Test Environments

All sites have QA instances that are sufficiently identical to production that the results of tests in QA can be relied on to evaluate the production instance.

Criticality Rating of Web Site(s)

Medium: The platform processes confidential and sensitive data, including FERPA-protected student education records and, where enabled, health-related assessment responses.

Database Protections

Web servers have defenses against typical attacks (such as SQL injection) via parameterized queries, stored procedures, or other techniques that do not pass arbitrary strings to the SQL command interpreter.

System Security

Proficiencee has been designed to achieve a high level of security by providing an uncomplicated, usable approach to user authentication, system access, and role-based, hierarchical permissions. Proficiencee is designed to support institution's own internal security policies and to provide rigorous protection from internal or external intrusions. Proficiencee reinforces system security by presenting a simple security model to end-users because research shows that if users have to jump through too many security hoops, they will attempt to find ways to bypass security entirely.

Identity and Access Management

Proficiencee Canvas supports centralized identity management and delegated authentication via integrations with external identity providers (IdPs) including Lightweight Directory Access Protocol (LDAP), Active Directory, Central Authentication Service (CAS), Security Assertion Markup Language (SAML) 2.0, and Shibboleth-compatible SAML federations. Proficiencee Canvas supports federated identity management and Single Sign-On (SSO) via these IdPs. Proficiencee LTI tools rely on the host LMS for authentication and accept signed LTI launches (LTI 1.1 / LTI Advantage as configured).

Proficiencee Canvas authentication can be used alone or concurrently with supported external IdPs. For example, when used with LDAP, Canvas presents credentials to the external IdP according to the configured authentication provider. If institutional SSO authentication fails, access is denied per institutional policy. Proficiencee LTI tools do not perform a separate password login; access requires a valid LTI launch from the LMS.

Where Proficiencee Canvas provides local (Canvas-native) authentication, passwords are never stored in plain text. Local passwords are securely hashed using a modern key derivation function (scrypt), with legacy SHA-512 hashes supported only for credential transition. When users authenticate via institutional SSO (SAML, CAS, LDAP, etc.), Proficiencee does not store the institution's directory passwords; authentication is delegated to the external identity provider. Proficiencee LTI tools do not store end-user passwords; those tools authenticate users via signed LTI launches from the LMS.

Protocol and Session Security

Proficiencee uses HTTPS (HTTP over TLS) for all communication. All inbound and outbound traffic is encrypted to ensure that all personally-identifiable information, credentials exchange, page requests, and session data are secure.

Sessions are maintained in the Proficiencee infrastructure and can be invalidated. The Canvas LMS platform uses encrypted session cookies with secure flags when SSL is forced. Proficiencee LTI tools use server-side Redis-backed sessions with a secure session cookie. Session IDs are validated against server-stored values. An invalidated session requires the user to authenticate again (via LMS login or a new LTI launch).

Sessions are reset on each successful login to prevent access to session IDs by subsequent logins. To prevent cross-site request forgery (CSRF) vulnerabilities, all user actions that modify data require a session secret key to post data. All requests that modify data are done with HTTPS POST or PUT requests, never GETs.

Preventing Cross-Site Scripting (XSS) Attacks

Proficiencee employs a variety of strategies to prevent cross-site scripting (XSS) attacks. For example, because user-supplied JavaScript presents a critical security vulnerability, Proficiencee does not allow non-administrative users to embed JavaScript directly into any Proficiencee pages. If, for example, a student were able to add JavaScript to a page, the student could embed code that changes the student's grade when the instructor visits the page without the instructor detecting it. For this reason, only Proficiencee account administrators can add custom JavaScript.

Proficiencee sanitizes content to protect against intentional or unintentional vulnerabilities. On the Canvas LMS platform, content entered through the Rich Content Editor is scrubbed server-side to remove malicious content. On Proficiencee LTI tools, user/instructor HTML is limited and sanitized on selected feedback and content paths. Content sanitization helps prevent session jacking, form hacks, and other unauthorized data access and/or modifications.

All user content is sanitized server-side — not in JavaScript, which can be bypassed — before it is saved to the database. The sanitization is done by explicit whitelisting, not blacklisting. This prevents the addition of JavaScript to HTML data and prevents the addition of unsafe HTML tags as well.

File Upload and Download Security

User-uploaded files on the Canvas LMS platform are stored in Amazon S3 with unique names and folders. Where configured, uploaded files are served from a separate files host/domain to take advantage of the browser's same-origin security measures and reduce session side-jacking risk. Proficiencee LTI tools store media such as videos in S3 (often via short-lived presigned upload URLs) and may deliver downloads (for example PDFs) using short-lived signed authorization tokens. All sensitive downloads should use unique, short-lived authorization keys.

Data Security

Proficiencee has developed custom code to validate that all Proficiencee data models are protected against invalid assignment. For example, no user can change foreign keys arbitrarily and all lookups are

scoped to the appropriate current user and context. All SQL is built using placeholders and a framework for escaping user input; strings are never directly interpolated or concatenated.

The Proficiencee Canvas platform provides a REST API protected by industry-standard OAuth2, allowing authorized applications to access data and perform actions without possession of the user's password; access can be revoked via developer keys / tokens. Proficiencee LTI tools expose a more limited API surface authenticated by application tokens (not a public third-party OAuth2 app store model) and return grades to the LMS via LTI Outcomes where configured.

Database Connection Security

Application servers communicate with the database via a database proxy that handles connection pooling. Connections are over a heavily firewalled virtual network.

Data Security through Redundancy and Versioning

To protect against malicious or accidental data destruction, Proficiencee stores data redundantly. On the Canvas LMS platform, soft-deletion patterns allow recovery of prior content states (for example assignments, submissions, and related gradebook data) according to Canvas workflows. Proficiencee LTI tools retain assessment attempt and response records in application databases; recovery depends on database backups rather than Canvas-style soft-delete UI for an LTI gradebook.

Proficiencee performs encrypted database backups on a daily basis. Backups are retained for 30 days and stored off-site in Amazon Web Services within U.S. regions for U.S. client institutions. Point-in-time recovery is available where enabled on the managed database service.

Internal Security

Proficiencee uses reasonable efforts to provide logical and physical security designed to maintain the integrity of its internal systems and customer data and content.

System and Data Access Policy

Proficiencee requires approvals for granting access to employees. A request is sent with detailed information about the level of access to the system and specifying which parts, functions, and features are to be accessible by the employee. Clear, valid, and necessary business justification must be provided for the user in question.

The completed access request is then reviewed by the direct manager of the requester. If management approves, the request is routed to the Operations team for final approval. If all parties approve the employee's access, the Operations team grants access. Per the employee exit policy, user accounts are deleted upon termination of employment.

All on-boarded Proficiencee employees are required to complete Family Educational Rights and Privacy Act (FERPA) training. https://studentprivacy.ed.gov/training/ferpa-101-colleges-universities

Cryptographic Keys

Proficiencee's Operations team controls generation and installation of keys for all employees with access to the servers. An automated configuration management system installs employee public keys on a per-server basis based on need. This same configuration process automatically revokes keys globally when necessary. Employees are required to use full-disk encryption and password protection on their work machines to protect their private keys and other sensitive data. The private keys used for HTTPS are stored in an encrypted form and decrypted by operations when deployed to the application servers.

Monitoring and alerts are in place to detect and warn of any changes to keys, users on the system, login and sudo attempts, and other events of concern.

Secure Coding and Development Practices

Maintaining and enhancing security is a disciplined, continual, and ongoing process. Secure coding and security testing are, therefore, integral components of Proficiencee's engineering and development methodology.

All Proficiencee developers are trained to identify and analyze security issues when writing and reviewing code. Members of the core security team and the engineering team subscribe to security-focused lists, blogs, and other resources to maintain, expand, and share the collective body of knowledge. The security and engineering teams keep up-to-date on general security practices, on recent attack vectors, and on any security issues specifically related to the languages, web applications, frameworks, and environments that Proficiencee employs to develop, host, and maintain Proficiencee.

Testing and Quality Assurance

New code is deployed to a continuous integration server where it is immediately tested. Proficiencee's testing team runs:

- Unit tests (testing code with code)
- Integration tests (testing code with integrations with other code)

After passing these tests, the code is incorporated in the main Proficiencee development code for formal quality assurance (QA). The QA team tests the new code on all supported platforms and browsers.

Proficiencee's Response to Security Alerts

Proficiencee is a cloud service with a single version of the code base and production environment so that security updates are immediately and automatically applied for the entire client base as part of Proficiencee's hosting services.

Regular vulnerability scans of the Proficiencee application and infrastructure are conducted using third-party tools (commercial vulnerability scanners), custom scripts, and open source tools. If any vulnerabilities are detected, Proficiencee's security and engineering teams work together to analyze, design, and develop the required patch. Security-related patches to the operating system, application software, and libraries are applied within one (1) week except in those cases which have been determined to be high severity. If a high-severity security vulnerability is detected, fixing the vulnerability is given the highest priority by Proficiencee's security and engineering teams. High-severity

security patches will be applied within twenty-four (24) hours by best commercial efforts. In most cases, the vulnerability can be fixed using a hot patch without incurring any downtime to the Proficiencee production environment.

Proficiencee, in coordination with AWS, relies on current AWS SOC / ISO compliance attestations (available via AWS Artifact) rather than legacy SAS 70 controls.

Operations, Privacy, and Accessibility

Availability and Disaster Recovery

Proficiencee targets 99% uptime for production services. Customers do not control the scheduling of planned maintenance windows. Proficiencee maintains a disaster recovery plan; disaster recovery components are tested approximately every six months. Some disaster recovery components may be located outside the United States as part of AWS regional redundancy; U.S. client production data remains hosted in U.S. AWS regions.

Privacy

Proficiencee maintains a privacy policy describing how personal and education data are handled. Privacy and legal terms are published at https://www.proficiencee.com/legal. Proficiencee does not sell student data and does not share institutional data with advertising platforms. Third-party subprocessors (for example AWS) are used to host and operate the service under contractual security obligations.

Accessibility

Accessibility is considered during content and software design for Proficiencee, including support for keyboard use and assistive technologies. Proficiencee aims to conform to the W3C Web Content Accessibility Guidelines (WCAG). A VPAT / accessibility statement is maintained at https://www.proficiencee.com/accessibility. Accessibility support is available through Proficiencee support channels (email, phone, and/or in-product chat where enabled), and instructors may escalate issues to their implementation support contact.

Information Security Program

Proficiencee designates personnel responsible for coordinating the information security program and maintains a documented information security policy and incident response plan. Administrative access is logged, and audit trails are retained for administrative actions. Security awareness training is mandatory for employees, and background screenings are performed as part of hiring practices. Intrusion detection and firewall controls are provided as part of the AWS-hosted architecture and Proficiencee operational monitoring.

LTI Integration Summary

Proficiencee LTI tools integrate with institutional LMSs (including Canvas) using LTI. Users are auto-provisioned from LTI launch data. Typical data transmitted and stored for the LTI tools include names, course/assignment context, and completion or assessment results for LTI-based assessments and guided

learning; grades may be passed back to the LMS via LTI Outcomes where configured. Proficiencee LTI tools do not require a separate end-user password. Proficiencee does not currently claim IMS Global certification for LTI 1.3 / LTI Advantage.

Incident and Vulnerability Notification

In the event of a security breach affecting customer data, Proficiencee will notify affected customers and describe the nature and scope of the incident. Material product vulnerabilities that require customer action or awareness are communicated to institutional LMS / technical contacts by email.

FERPA

Proficiencee was built to comply with the Family Educational Rights and Privacy Act (FERPA) by design, and Proficiencee readily integrates with the school's LMS using the Learning Tools Interoperability (LTI) protocols to prevent unauthorized access to FERPA-protected data. Proficiencee provides educational institutions and agencies with multiple mechanisms and technologies to manage, enforce, and comply with the provisions of FERPA and to fulfill their responsibilities under its requirements.

FERPA Overview

FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools and institutions that receive funds under the applicable program of the U.S. Department of Education. FERPA provides students, and in some instances parents, the right to inspect their education records and some ability to control the disclosure of information contained in their education records.

FERPA requires educational agencies, which disclose personally identifiable information from a student's education record to other school officials, to use "reasonable methods" to insure school officials obtain access to only the education records they have legitimate educational interests in.

Table 6–1 identifies key sections and requirements of the Family Educational Rights and Privacy Act (FERPA) and briefly describes how Proficiencee (Canvas LMS platform and LTI tools) complies.

Table 6–1. Key FERPA Requirements and Proficiencee Compliance

Item	FERPA Section	Requirements	Comments
Agency or Institution Disclosure to Proficiencee as a "School Official"	34 CFR § 99.31 (a)(ii)	Education institution must use "reasonable methods" to make sure school officials have access to only education records they have legitimate educational interests in.	Provide Proficiencee only the information needed to serve its function. Access to educational records is dictated by course enrollment and role data provided by the institution. Access inside of a course can be further limited by

Item	FERPA Section	Requirements	Comments
			groupings of students.
Requirement of Further Non-Disclosure	34 CFR § 99.33 (a)(1)	School can disclose information only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.	Contract with Proficiencee specifies that Proficiencee not disclose the information to any other party and otherwise in compliance with FERPA.
Permission settings within the Software	34 CFR § 99.30 (a)	Parent or eligible student shall provide a signed & dated written consent before an educational agency or institution discloses personally identifiable information from the student's educational records, except as provided in § 99.31.	Agency or institution can change the permissions settings within the software to allow for, or deny, access to certain types of users.
Course Settings	Same as above	Same as above	Agency or institution can change the course settings within the software to allow certain users to access the course.
Account Settings	Same as above	Same as above	Agency or institution can change the account settings within the software to allow only certain users to access features.
Names, not potentially sensitive contact information, are displayed in Proficiencee (security feature)	Same as above	Same as above	Proficiencee displays students' names in the course; however students' email addresses or phone numbers will not be displayed. Students enrolled in the same course can contact one another, but the communication will be mediated through

Item	FERPA Section	Requirements	Comments
			Proficiencee and students' email addresses will not be disclosed.
Log off inactive users (security feature)	Same as above	Same as above	Proficiencee automatically logs out users after a period of inactivity.
Browser Session Log out (security feature)	Same as above	Same as above	Once a browser session is closed and a new browser is opened, Proficiencee will require the user to login again.
Authentication Integration	Same as above	Same as above	Single-sign-on is highly encouraged. All access to the system is dictated by the Institution-controlled identity system (SAML 2.0, CAS, LDAP, Shibboleth etc.).

Customization

Under FERPA, each school must define in their annual notification who constitutes a school official and what constitutes a legitimate educational interest. Because of this variation, Proficiencee provides settings that can be configured to conform to each school's definitions. This document describes the various Proficiencee settings related to FERPA, the default settings, and the changes that may be made to these settings.

Permissions

One of the main FERPA-related tools available to educational agencies is the ability to define the permission settings for specific user roles in Proficiencee. Roles are established and communicated within Proficiencee by the type of course or section enrollment. The management of enrollments and the associated role permissions enable schools to specify what data each user can view. Both instructor and teacher's assistant enrollments can be limited to student data in a section, which is a sub-group of the overall course enrollments. Enrollment data is typically furnished via LTI integration. The default permission settings can be changed to either allow or deny access to specific features and data.

Course Settings

All data and course content is securely stored under an associated access control policy. Every time the data or content is accessed, this access control policy is consulted before access is granted to the requested resource. By default, Proficiencee only allows users enrolled in a course to view course

content. With the growing need for OpenCourseWare and open educational resources, Proficiencee, through the mechanism of these access control policies, can safely permit the sharing of course content publicly while protecting and maintaining the privacy of all personal and FERPA-associated content. These policies support the sharing of continuously updated course content without compromising data security.

Authentication Integration

Single Sign-On (SSO) is configured at the Canvas account level and gives the institution control over which users are authenticated and how. Role and enrollment data are communicated via SIS and/or LTI. Supported Canvas identity protocols include LDAP, Active Directory, CAS, SAML 2.0, and Shibboleth-compatible SAML. Proficiencee LTI tools inherit authentication from the launching LMS via LTI.

Assessment Results in External Notifications

An educational agency can decide whether or not it will allow students to have the ability to opt-in to receiving grades by external notifications through email, SMS, or other communication channels. By default, when an instructor assesses submitted assignments, students can receive notifications that they have received a grade on a specific assignment, but the notification will not include the grade received. If the educational agency has selected this option, it will allow the student to consent or opt-in to receive the grade in the notification as well.

Other Default FERPA-related Features

Additional features in Proficiencee related to FERPA compliance include:

- **Inactive user logout.** Proficiencee will automatically logout the user after a period of inactivity.
- **Browser session logout.** Once a browser session is closed and a new browser session is opened, Proficiencee will require the user to login again.
- **Protection of sensitive contact information.** Although Proficiencee displays students' names, Proficiencee will not display students' email addresses, phone numbers, and other sensitive contact information to other students. Proficiencee mediates communications, allowing users enrolled in the same course to contact one another without the disclosure of users' actual contact information. Administrators with the appropriate permissions can access the audit and record of Proficiencee communications.