AEC Academia Security Overview

Last Updated: February 20, 2026

Prepared by:
ATL Software LLC
Publisher of the AEC Academia software platform
7901 4th Street North, Suite 300
St. Petersburg, FL 33702
United States
info@aec.app
www.aec.app

1. Purpose

This document provides customers and prospective customers of AEC Academia with a high-level overview of the security measures implemented by ATL Software LLC to protect customer data and ensure the secure operation of the AEC Academia platform.

The objective of this document is to describe the principal administrative, technical, and organizational safeguards used to secure the platform without disclosing confidential implementation details.

2. Scope

This document applies to the AEC Academia SaaS platform, including web applications, APIs, customer databases, document storage, supporting infrastructure, software development processes, and operational support activities.

3. Security Governance

ATL Software LLC is responsible for the security and operation of the AEC Academia platform. Security is managed through a combination of technical controls, operational procedures, infrastructure protections, and continuous improvement activities.

4. Hosting Infrastructure

AEC Academia is hosted on dedicated OVHcloud bare-metal servers located in Canada, France, and Singapore. Hosting locations are selected according to customer geographic requirements.

Customer environments operate on dedicated physical infrastructure that is not shared with other customers.

5. Customer Data Isolation

Each customer operates within its own dedicated application environment and database structure. Customer databases are separated on a per-customer basis and environments operate independently from one another.

6. Authentication and Access Control

User authentication is performed through secure login mechanisms. Passwords are stored using industry-standard secure hashing techniques.

Multi-Factor Authentication (MFA) is supported by the platform and may be enabled or enforced by customer organizations.

Administrative access to production infrastructure is restricted to authorized personnel. Access rights are removed promptly when personnel leave the organization or no longer require access.

7. Personnel Security

Employees and contractors with access to confidential information are subject to confidentiality obligations. Access to sensitive information is limited to personnel who require such access to perform their responsibilities.

8. Network Security

AEC Academia benefits from multiple layers of network protection, including firewall controls, OVHcloud Anti-DDoS services, and Cloudflare Web Application Firewall (WAF) protection.

These controls help reduce the risk of unauthorized access, malicious traffic, and denial-of-service attacks.

9. Data Protection

All communications between users and the platform are protected using HTTPS/TLS encryption.

Production backups are encrypted before being transferred to secure offsite storage locations hosted by Amazon Web Services (AWS).

10. Logging and Audit Trail

AEC Academia maintains authentication logs and application audit records to support operational monitoring, troubleshooting, support activities, and security investigations.

User authentication events and key application activities are recorded and may be reviewed by authorized ATL Software personnel when required.

11. Secure Software Development

Source code is maintained in Bitbucket version-controlled repositories.

Development, testing, and pre-production environments are separated from production systems.

Changes are validated through a combination of unit testing, automated testing, and manual testing before deployment.

Deployments are automated and executed through controlled release processes initiated by authorized personnel.

12. Vulnerability and Patch Management

Operating system updates, security patches, and infrastructure maintenance activities are applied on a regular basis as part of ongoing platform operations.

13. Backup and Recovery

AEC Academia uses a multi-layered backup strategy combining database replication and daily offsite backups.

Production data is replicated to secondary infrastructure and backed up daily to Amazon Web Services (AWS). Backup data is retained for up to 18 months.

Backup restoration procedures are regularly performed as part of operational support and incident investigations.

In the event of a major infrastructure failure, ATL Software aims to restore services within a typical recovery window of up to 24 hours, depending on the nature and scope of the incident.

14. Monitoring and Availability

The platform is continuously monitored using automated monitoring systems. Operational alerts enable rapid identification and response to service disruptions, infrastructure failures, and abnormal behavior.

15. Incident Response

ATL Software follows a structured incident response approach designed to contain risks, restore services, and minimize customer impact.

Incidents are assessed as soon as they are detected. The team analyzes the situation, isolates affected systems when necessary, identifies root causes, implements corrective actions, and restores services using established recovery procedures.

When an incident is likely to affect customers or customer data, affected customers are informed as early as practical and updated until resolution.

16. Subprocessor Management

AEC Academia uses a limited number of carefully selected third-party service providers. Details regarding subprocessors used in connection with the platform are maintained in the AEC Academia Subprocessor List.

17. Continuous Improvement

ATL Software continuously reviews and improves security controls, infrastructure protections, operational procedures, monitoring capabilities, and incident response processes in order to maintain a secure and reliable SaaS platform.

18. Contact Information

For questions regarding information security, customers may contact ATL Software LLC at info@aec.app.