Service Continuity & Incident Management 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

Client-facing overview of service continuity, incident management, and recovery objectives

1. Purpose of This Document

This document provides AEC Academia clients with a clear and transparent overview of how ATL Software ensures service continuity in the event of an incident.

Its objective is to explain, at a high level and without disclosing confidential technical details:

- How incidents are managed and communicated
- How data and services are recovered
- What recovery objectives (RTO / RPO) are applied

This document describes how ATL Software operates a structured, reliable, and professionally managed SaaS platform, aligned with recognized industry best practices.

2. Scope

This document applies to the AEC Academia SaaS platform, including:

- Application services (web interface, APIs)
- Databases and client data
- Supporting infrastructure required for normal service operation

It covers incidents that may impact service availability, data integrity, or security.

3. Types of Incidents Covered

ATL Software maintains procedures to manage the following categories of incidents:

- Infrastructure or hosting outages
- Network or connectivity disruptions
- Cybersecurity incidents (e.g. attempted intrusion, denial-of-service attacks)
- Software failures or critical bugs
- Data corruption or accidental data loss

Each incident is assessed, classified by severity, and handled according to predefined internal procedures.

4. Incident Management Governance

Incident management within ATL Software is coordinated through a clear governance structure:

- **Incident Coordination:** Led by senior technical staff with decision-making authority
- **Technical Resolution:** Handled by the development and infrastructure teams
- **Client Communication:** Coordinated by the support team, with validated information

All incidents follow a structured lifecycle:

1. Detection and confirmation
2. Impact assessment and prioritization
3. Containment and corrective actions
4. Service restoration
5. Post-incident review and improvement

5. Client Communication During an Incident

ATL Software considers transparent and timely communication to be a critical part of incident management.

5.1 Initial Notification

In the event of a significant service disruption:

- Clients are informed as soon as the incident is confirmed
- Initial communication typically occurs within **2 to 4 hours**, depending on incident severity

5.2 Communication Channels

Clients may be informed through one or more of the following channels:

- Email notifications
- Customer support communications
- Status updates provided by the support team

5.3 Ongoing Updates

During prolonged incidents:

- Regular updates are provided with the latest available information
- Updates focus on service impact, progress toward resolution, and estimated restoration timelines

6. Hosting, Infrastructure & Data Protection

This section provides concrete and transparent information for IT and security teams regarding how AEC Academia is hosted, protected, and backed up.

6.1 Hosting Environment & Data Location

AEC Academia is hosted on **dedicated physical servers** operated by **OVH** in professional data centers.

- Instances are deployed in OVH data centers located in:
  - **Canada**
  - **France (Europe)**
  - **Singapore (Asia)**
- The hosting location is selected according to the geographic location of the client in order to optimize performance and comply with data residency expectations.

The servers used for AEC Academia are:

- **Physical (bare-metal) servers**
- **Not virtualized**
- **Not shared with other customers**

This architecture eliminates risks related to multi-tenant virtual environments and provides strong isolation between client instances.

6.2 Physical Security & Data Center Protection

OVH data centers implement strong physical security measures, including:

- 24/7 video surveillance
- Badge-based and biometric access controls
- Restricted access zones
- On-site security personnel
- Fire detection and automatic fire suppression systems
- Power redundancy and backup generators

ATL Software does **not** require permanent physical access to servers. All operations are performed through secure remote access mechanisms.

7. Infrastructure Resilience & Network Security

7.1 Hardware Resilience

At the server level, the dedicated physical servers used by AEC Academia are configured with **redundant hardware architectures**, including:

- **RAID 1 disk mirroring**, which protects data against individual disk failures
- **Redundant power supplies (dual PSU)**, ensuring continued operation in case of power supply failure

These hardware-level redundancies significantly reduce the risk of service disruption caused by single-component failures.

7.2 Network Protection

AEC Academia benefits from multiple layers of network protection designed to ensure high availability and resilience:

- **Firewall protection** to control and restrict network traffic
- **Anti-DDoS protection**, designed to absorb and mitigate large-scale traffic attacks intended to disrupt service availability
- **Cloudflare protection**, which acts as a global security and traffic filtering layer in front of the platform

Cloudflare helps protect AEC Academia by:

- Filtering malicious traffic before it reaches servers
- Blocking automated attacks and suspicious requests
- Mitigating denial-of-service attacks
- Improving availability and performance through a global network

These protections reduce the risk of service disruption and unauthorized access.

8. Backup Strategy & Data Protection

ATL Software operates a structured and robust backup strategy using **Amazon Web Services (AWS)**.

Backup Storage Locations

Backups are stored in geographically separated AWS regions:

- **Europe:** Paris, Dublin
- **United States:** Texas
- **Asia:** Singapore

This geographic distribution protects client data against regional outages or physical incidents.

Backup Frequency & Retention

- **Backup frequency:** Daily (performed during night hours)
- **Retention policy:**
    - Daily backups retained for the last **7 days**
    - Weekly backups retained for the following **30 days**
    - Monthly backups retained for **18 months**

Encryption & Protection

- All backups are **encrypted** using industry-standard encryption mechanisms
- Backups are protected by AWS against accidental deletion
- Access to backup data is strictly restricted

Backup Validation

- Backup integrity and restorability are periodically tested

9. Server Failure & Recovery Scenarios

AEC Academia is hosted on dedicated physical servers located within OVH data centers. As such, hardware-level incidents are handled in close coordination with OVH's on-site technical teams.

Physical Server Incident Handling

OVH provides continuous hardware monitoring and on-site intervention. In most physical hardware incidents, an on-site technician intervenes within approximately one hour, depending on the nature of the issue and support conditions.

In the event of a physical hardware issue (disk failure, power supply issue, motherboard fault, etc.):

- OVH continuously monitors the physical infrastructure and detects hardware anomalies automatically
- Once a physical issue is detected, OVH dispatches a qualified technician directly to the server rack
- The technician performs on-site diagnostics, hardware replacement if necessary, and server restart
- This physical intervention typically takes **less than one hour**

During this process, ATL Software coordinates with OVH support to monitor progress and validate service restoration.

Alternative Recovery Scenario

If the affected server cannot be repaired within a reasonable timeframe or is deemed non-recoverable:

- ATL Software activates an alternative dedicated server available within OVH infrastructure
- The affected instance is redeployed on the new server
- The most recent valid encrypted backup is restored from AWS

In this scenario, full service restoration typically occurs within **30 minutes to 1 hour**, depending on the incident scope.

This dual recovery approach ensures both rapid physical intervention and a reliable fallback strategy in case of major hardware failure.

10. Incident Scenarios & Operational Response

This section outlines how ATL Software responds to concrete operational scenarios.

10.1 Infrastructure or Hosting Outage

Scenario: Server, network, or hosting provider outage

Actions executed by ATL Software:

- Detection through monitoring alerts
- Incident confirmation and impact assessment
- Engagement with the hosting provider
- Restoration of services using available infrastructure resources
- Client communication during the incident

10.2 Data Loss or Corruption

Scenario: Accidental deletion, corruption, or system failure

Actions executed by ATL Software:

- Identification of affected data scope
- Isolation of impacted systems if required
- Restoration from encrypted backups
- Verification of restored data

10.3 Cybersecurity Incident

Scenario: Suspicious activity, attempted intrusion, or denial-of-service attack

Actions executed by ATL Software:

- Traffic filtering and blocking at the network level
- Isolation of affected components
- Security analysis and corrective actions
- Reinforcement of controls where necessary

10.4 Environmental or Physical Incident

Scenario: Fire, power failure, or physical security incident at the data center

Actions executed by ATL Software:

- Reliance on data center protection systems (fire suppression, power redundancy)
- Service restoration following provider recovery procedures
- Data recovery from offsite backups if required

11. Recovery Objectives (RTO & RPO)

ATL Software defines realistic recovery objectives aligned with the operational model of a PME SaaS platform.

11.1 Recovery Time Objective (RTO)

- **Target RTO:** Up to **24 hours** for full service restoration after a critical incident
- Partial restoration may occur earlier depending on incident nature

11.2 Recovery Point Objective (RPO)

- **Target RPO:** Up to **24 hours**
- In worst-case scenarios, data recovery is limited to the most recent daily backup

12. Business Continuity Measures

ATL Software implements multiple continuity measures to minimize disruption and protect client data.

12.1 Data Backup and Protection

- Regular automated backups of critical data
- Encrypted backup storage
- Secure offsite backup locations
- Periodic backup integrity testing

12.2 Infrastructure Protection

- Professionally hosted infrastructure in certified data centers
- Network protection, firewalls, and DDoS mitigation
- Secure encrypted communications (TLS)
- Continuous system monitoring

12.3 Secure Development and Operations

- Security-by-design principles
- Controlled deployment processes
- Continuous monitoring and patch management

13. Client Support During Incidents

During service disruptions:

- The support team remains available to handle client requests
- Requests are prioritized based on severity and impact
- Clear and consistent information is provided to clients

ATL Software's objective is to minimize operational impact for clients and restore normal service conditions as quickly as possible.

14. Post-Incident Review and Continuous Improvement

After any major incident, ATL Software conducts a structured internal review to:

- Identify root causes
- Validate the effectiveness of response actions
- Implement corrective and preventive measures

Lessons learned are incorporated into:

- Updated procedures
- Improved monitoring and controls
- Enhanced communication processes

15. Information Security Alignment & Commitment

This document is complementary to ATL Software's internal Information Security policies and procedures.

While detailed technical and security controls are not disclosed for confidentiality reasons, ATL Software confirms that:

- Information security and business continuity are managed within a structured governance framework
- Policies are reviewed regularly and aligned with recognized industry best practices

ATL Software is committed to providing a reliable, secure, and professionally managed SaaS platform.

Service continuity and client trust are considered strategic priorities, and continuous improvement remains a core principle of our operations.

16. Contact Information

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