AWARELY LEARNING

Cybersecurity awareness training platform

Security & Trust Overview

Awarely Learning — controls, operational practices and limits

Generated: 2026-07-17

> This document summarises the security controls, operational practices and limits of the Awarely Learning platform as implemented in the product. We provide a platform for managing training and the associated records; we do not turn technology into a compliance guarantee or a security guarantee. Certifications and production controls are validated separately, on request.

1 Authentication and access control

- Authentication via Amazon Cognito (AWS), with a forced password change on first sign-in.
- Multi-factor authentication (MFA) via TOTP.
- Role-based access control (RBAC): learner, viewer, manager, org-admin, billing-admin, superadmin.
- SSO configurable per organization, where required.

2 Multi-tenant isolation

- Organizations are logically isolated; data and administration are separated per organization.

3 Data and content protection

- Hosted in the European Union (AWS region eu-central-1, Frankfurt).
- Encryption at rest via managed AWS services (S3, DynamoDB); keys managed with AWS KMS where configured.
- Access to protected media through time-limited signed URLs.
- Video player with forward-seek prevention to support full viewing.
- Certificates with a publicly verifiable QR code at the /verify route.

4 Upload security (SCORM)

- Every uploaded SCORM package is scanned for malware (Amazon GuardDuty Malware Protection for S3).

- Structural archive validation before serving (file count, total size, compression ratio, path traversal, manifest presence) — zip-bomb-safe by construction, without decompressing any entry.
- Content is not served until its status is “validated”; rejected packages are handled accordingly.

5 Operational integrity

- Audit log for important platform operations.
- External effects (email, PDF generation) use a durable intent model for exactly-once delivery and reconciliation.
- Monitoring and alarms for critical operations and for stuck intents.

6 Resilience and availability

- Documented backup and restore procedure (restore drill).
- Installable application (PWA) with an offline shell for the core interface.

7 Accessibility

- Target compliance with WCAG 2.1 levels A and AA on public and authenticated pages, with automated scans (axe-core) in the pipeline. Automated checks cover machine-detectable issues; manual review still applies.

8 Privacy and compliance

- Public documents: Terms & Conditions, Privacy Policy and Data Processing Addendum (DPA).
- Processing of personal data in accordance with the GDPR; DPA available for organizations.
- The platform can support awareness programmes and training records for initiatives such as NIS2, but compliance depends on each organization’s controls, processes and obligations.

9 What we do not claim (transparency)

- At this time we do not claim formal certifications such as SOC 2 or ISO 27001. Any such status will be communicated explicitly once obtained.
- The platform does not provide a compliance guarantee and no public SLA is defined; these are discussed contractually, on request.

10 Contact and resources

- For security requirements, due diligence or technical evaluation: learning@awarely.ro.

- Online resources: /security, /technical-overview, /buyer-due-diligence, /dpa.

This document reflects the practices implemented as of the generation date and is informational; it does not constitute a contractual guarantee. Production, contractual and support details are confirmed directly.