



Prezentare Securitate și Încredere

Security & Trust Overview — controale, practici operaționale și limite

Generat: 2026-07-17

Acest document rezumă controalele de securitate, practicile operaționale și limitele platformei Awarely Learning, așa cum sunt implementate în produs. Oferim o platformă pentru administrarea trainingului și a evidențelor asociate, fără a transforma tehnologia într-o garanție de conformitate sau de securitate. Certificările și controalele de producție se validează separat, la cerere.

1 Autentificare și control al accesului

- Autentificare prin Amazon Cognito (AWS), cu forțarea schimbării parolei la prima autentificare.
- Autentificare multi-factor (MFA) prin TOTP.
- Acces bazat pe roluri (RBAC): cursant, viewer, manager, org-admin, billing-admin, superadmin.
- SSO configurabil per organizație, unde este solicitat.

2 Izolare multi-tenant

- Organizațiile sunt izolate logic; datele și administrarea sunt separate per organizație.

3 Protecția datelor și a conținutului

- Găzduire în Uniunea Europeană (regiune AWS eu-central-1, Frankfurt).
- Criptare în repaus prin serviciile AWS gestionate (S3, DynamoDB); chei gestionate prin AWS KMS unde este configurat.
- Acces la conținutul media protejat prin URL-uri semnate, cu durată limitată.
- Player video cu prevenirea derulării înainte, pentru a susține vizionarea completă.
- Certificate cu cod QR verificabil public la ruta /verify.

4 Securitatea încărcărilor (SCORM)

- Fiecare pachet SCORM încărcat este scanat antimalware (Amazon GuardDuty Malware Protection for S3).
- Validare structurală a arhivei înainte de servire (număr de fișiere, dimensiune totală,



rată de compresie, path traversal, prezența manifestului) — rezistentă la zip-bomb prin construcție, fără decompimarea intrărilor.

- Conținutul nu este servit până când nu are statusul „validat”; pachetele respinse sunt tratate corespunzător.

5 Integritate operațională

- Jurnal de audit pentru operațiunile importante ale platformei.
- Efectele externe (email, generare PDF) folosesc un model de intenție durabilă pentru livrare exactly-once și reconciliere.
- Monitorizare și alarme pentru operațiuni critice și pentru intențiile rămase blocate.

6 Reziliență și disponibilitate

- Procedură de backup și restore documentată (restore drill).
- Aplicație instalabilă (PWA) cu shell offline pentru interfața de bază.

7 Accesibilitate

- Țintă de conformitate WCAG 2.1 nivel A și AA pe paginile publice și autentificate, cu scanări automate (axe-core) în pipeline. Verificarea automată acoperă problemele detectabile automat; revizuirea manuală rămâne aplicabilă.

8 Confidențialitate și conformitate

- Documente publice: Termeni și Condiții, Politica de Confidențialitate și Anexa de Prelucrare a Datelor (DPA).
- Prelucrarea datelor cu caracter personal în conformitate cu GDPR; DPA disponibil pentru organizații.
- Platforma poate susține programe de awareness și evidențe de training pentru inițiative precum NIS2, însă conformitatea depinde de controalele, procesele și obligațiile fiecărei organizații.

9 Ce nu pretindem (transparență)

- La acest moment nu declarăm certificări formale de tip SOC 2 sau ISO 27001. Orice astfel de statut va fi comunicat explicit atunci când va fi obținut.
- Platforma nu oferă o garanție de conformitate și nu este definit un SLA public; acestea se discută contractual, la cerere.

10 Contact și resurse

- Pentru cerințe de securitate, due diligence sau evaluare tehnică: learning@awarely.ro.
- Resurse online: [/security](#), [/technical-overview](#), [/buyer-due-diligence](#), [/dpa](#).



Acest document reflectă practicile implementate la data generării și are caracter informativ; nu constituie o garanție contractuală. Detaliile de producție, contractuale și de suport se confirmă direct.

