
— SECURITY DOSSIER

Whiteboard security dossier

Hosting, isolation, identity, encryption, continuity, sub-processors, assessment and legal framework: the answers to hand to your CISO, verifiable in the product and its documentation.

On one page

Hosting	Hetzner Online GmbH, Germany (EU); in Morocco on request (dedicated instance).
Isolation	PostgreSQL row-level security ENABLE + FORCE on every table, application role NOSUPERUSER NOBYPASSRLS.
Identity	SAML 2.0, OpenID Connect, Entra ID, Google; SCIM 2.0; enforceable TOTP MFA; configurable idle timeout.
Traceability	Append-only audit log (PostgreSQL trigger), retention from 1 to 10 years.
Encryption	TLS + HSTS; secrets encrypted in the database; AES-256 encrypted backups; expiring signed links.
Continuity	pgBackRest PITR; timed drill on 10/10/2026; objectives RPO 15 min, RTO 4 h.
Reversibility	Full export: NDJSON, files, IMS Common Cartridge courses.
Assessment	Internal OWASP ASVS 4.0.3 level 2 self-assessment; external penetration test scheduled; no certification claimed.

01 · HOSTING

A named host. A Morocco option.

Hetzner, in Germany

The service is hosted by Hetzner Online GmbH, in a data centre in Germany, in the European Union.

A written move

Relocation is a written, rehearsed procedure: a restore on the new servers, then a DNS switch, during an announced maintenance window of one to three hours.

In Morocco on request

The same application image runs at a Moroccan host: it needs only containers, PostgreSQL and S3-compatible storage. Dedicated instance, Enterprise plan.

No proprietary service

No managed database, no cloud vendor's message queue: queues, cache and jobs run inside PostgreSQL. Nothing ties you to one host.

02 · ISOLATION

Each customer is isolated by the database itself.

Most multi-tenant platforms isolate customers in application code. We do too, and PostgreSQL enforces it underneath.

Row-level security, forced

Every table carries the organisation's ID, with `ENABLE` and `FORCE ROW LEVEL SECURITY`: a policy rejects any row of another organisation, even for the tables' owner.

✓ Proven at every release

An automated test fails if a table is unprotected or if a cross-customer read becomes possible.

An unprivileged role

The application connects with a role that is neither superuser nor `BYPASSRLS`; the production setup script stops if it is.

Content on a separate origin

SCORM packages and uploaded HTML are served from a separate subdomain, out of the session cookie's reach; files through signed links valid for five minutes.

03 · IDENTITY AND ACCESS

SSO, SCIM, MFA, sessions: what your policy requires.

Single sign-on

SAML 2.0, OpenID Connect, Microsoft Entra ID or Google, with accounts created at first sign-in.

Enforceable MFA

One-time codes (TOTP), enforceable for administrators — on by default for a new workspace — or for all staff. With SSO, your identity provider's MFA applies.

Passwords

Argon2id hashing; a fifteen-minute lockout after five failures.

SCIM 2.0 provisioning

Accounts created, updated and suspended from your directory.

Idle timeout

Set per organisation: 30 minutes by default for administrators, 8 hours for everyone else. Sessions bound to the device and revocable.

Controlled support access

Read-only, with your approval, seven days at most; every read is written to your audit log.

04 · TRACEABILITY

An append-only log, protected by the database.

Sign-ins, accounts, roles, exports, views of individual data, support access: every sensitive action is recorded with its author, target and changes. A PostgreSQL trigger rejects any update or deletion; only the purge at the retention period you set touches it.

- ✓ Author, target, changes
- ✓ Updates rejected by the database
- ✓ Retention from 1 to 10 years (2 years by default)

05 · ENCRYPTION

Encrypted in transit, secrets encrypted at rest.

 In transit

HTTPS everywhere, two-year HSTS, Let's Encrypt certificates renewed automatically.

 Encrypted backups

Encrypted by the backup tool (AES-256) before they are written to the repository.

 Encrypted secrets

MFA keys, SSO secrets, signing keys and integration tokens are encrypted in the database by the application.

 Signed links

No file is publicly accessible: every download goes through a signed link that expires.

06 · CONTINUITY

Backed up, restored, timed.

 Point-in-time recovery

Transaction log archived continuously (pgBackRest), a full backup on Sundays, differential the other nights, four weeks of history.

 15 minutes, 4 hours

Our objectives: at most 15 minutes of data lost, service back within 4 hours. The drill is scheduled monthly in production.

 A timed drill

On 10 October 2026: a 173 MB database restored to a precise point in time in about thirty seconds, end to end; 126,086 grades out of 126,086 recovered.

 A second host

Before any real data, the backup repository sits with a second hosting provider, separate from the first.

07 · SUB-PROCESSORS

Who processes your data, and when.

AI can be switched off per organisation, feature by feature or entirely. On an instance in Morocco, data and backups stay in Morocco; AI and e-mail delivery are then the only services outside Morocco, and each can be switched off or replaced.

SUB-PROCESSOR	ROLE	LOCATION	WHEN
Hetzner Online GmbH	Hosting: servers, database, files, backups.	Germany (EU)	Always
OpenAI or Anthropic (one only)	AI features. People are referred to by pseudonymous IDs; under the provider's API terms, the data sent is not used to train its models.	United States	If AI is on
Let's Encrypt (ISRG)	HTTPS certificates. Receives domain names only, no personal data.	United States	Always
E-mail delivery provider	Invitations, notifications and scheduled reports by e-mail. Named in the data processing agreement.	Named in the contract	If e-mail is on
Meta (WhatsApp Business)	WhatsApp reminders, only to people who accepted them.	Per Meta	If you turn it on

08 · REVERSIBILITY

Leave with everything, at any time.

Your administrator generates a complete archive: every table as NDJSON, the files, every course as IMS Common Cartridge, a manifest and instructions in three languages. A signed link valid for 24 hours, a logged download, the archive deleted after seven days.

- ✓ Open formats
 - ✓ Courses that re-import into another platform
 - ✓ No exit fee
-

09 · ASSESSMENT

What we have checked, and what remains.

- An internal self-assessment against OWASP ASVS 4.0.3, level 2, dated 10 October 2026: 160 requirements met, 10 partially, 25 not applicable. It is our own review, not an audit.
 - An external penetration test is scheduled before going live with real data. Its statement of work is written.
 - At every release: isolation tests between customers, a permission matrix for every role, static security analysis, dependency audit and secret scanning.
 - We hold no ISO 27001 certification and no SOC 2 report, and do not claim otherwise.
-

10 · LEGAL FRAMEWORK

Law 09-08, Law 05-20 and your obligations.

- Law 09-08: you are the data controller, we act as processor, under a data processing agreement.
 - For your workspace, the platform prepares the record of processing, a draft CNDP declaration, the processing agreement, the list of sub-processors and the retention periods, for your lawyer to approve.
 - Configurable retention periods; export and anonymisation on request — anonymisation keeps grades for your statistics.
 - Law 05-20: if your obligations require national hosting, a dedicated instance in Morocco meets them, to be confirmed with your CISO.
-

11 · BANKING

Outsourcing in the banking sector.

A bank that entrusts a service to a provider must be able to locate it, control it and leave it. The service can be hosted in Morocco, on an instance dedicated to you. The contract provides for your right to audit and for reversibility, with the full export described above.

- ✓ Hosting in Morocco available
 - ✓ Right to audit in the contract
 - ✓ Reversibility in the contract
-

Questions from your CISO

Your organisation's security questionnaire, an architecture review or access to the detailed self-assessment: write to us.

contact@whiteboard.ma

Whiteboard · whiteboard.ma · Version of 15 October 2026