Public technical and organizational measures NeuroDisplay

Version: tom-2026-08-en-v1

Effective date: 2026-08-01

sha256:e546ab492888b0f266b293c61b594004d09b497f2a9b3c57b7f6d00ed7a410e7

This document describes established controls. It constitutes neither a certification nor a guarantee of absolute security.

1. Governance and access

Individual access, RBAC, role management, server controls, review of authorizations and separation of tasks according to operational needs.

2. Isolation and authorization

RLS, multi-tenant isolation, cross-org controls, allowing Player commands, and server-side denial of out-of-scope operations.

3. Secrets and encryption

Secrets kept on the server side, no secrets in the frontend, encryption in transit and encrypted storage according to the providers' capabilities. Access to private objects uses temporary signed URLs when required.

4. Logging and minimization

Request_id, redacted logs, limited durations, absence of prompts in Analytics, separation of technical evidence and business content.

5. Environments and tests

Test/Production separation, synthetic fixtures, dedicated sandbox organizations, protections for real organizations and absence of cross-org mutation in tests.

6. Availability and backups

Backups and continuity according to suppliers' capacities and technical cycles. Backups are not reused for business purposes and deletions are reapplied after restoration when required.

7. Incidents and suppliers

Incident procedure, controlled preservation of evidence, notification of the Customer without undue delay, rate limiting, monitoring of suppliers and applicable contractual transfer mechanisms.