Mesures techniques et organisationnelles publiques NeuroDisplay

Version: tom-2026-08-v1

Effective date: 2026-08-01

sha256:1a644b47539b4e36d2250db09198135dadde733ea432d1e0c72a39f047a0f04e

Le présent document décrit des contrôles établis. Il ne constitue ni une certification ni une garantie de sécurité absolue.

1. Gouvernance et accès

Accès individuels, RBAC, gestion des rôles, contrôles serveur, revue des habilitations et séparation des tâches selon les besoins opérationnels.

2. Isolation et autorisation

RLS, isolation multi-tenant, contrôles cross-org, autorisation des commandes Player et refus côté serveur des opérations hors périmètre.

3. Secrets et chiffrement

Secrets conservés côté serveur, aucun secret dans le frontend, chiffrement en transit et stockage chiffré selon les capacités des fournisseurs. Les accès aux objets privés utilisent des URLs signées temporaires lorsqu'elles sont requises.

4. Journalisation et minimisation

Request_id, journaux expurgés, durées bornées, absence de prompts dans les Analytics, séparation des preuves techniques et du contenu métier.

5. Environnements et tests

Séparation Test/Production, fixtures synthétiques, organisations sandbox dédiées, protections des organisations réelles et absence de mutation cross-org dans les tests.

6. Disponibilité et sauvegardes

Sauvegardes et continuité selon les capacités et cycles techniques des fournisseurs. Les sauvegardes ne sont pas réutilisées à des fins métier et les suppressions sont réappliquées après restauration lorsque requis.

7. Incidents et fournisseurs

Procédure d'incident, conservation contrôlée des preuves, notification du Client sans retard injustifié, rate limiting, suivi des fournisseurs et mécanismes contractuels de transfert applicables.