Öffentliche technische und organisatorische Maßnahmen NeuroDisplay

Version: tom-2026-08-de-v1

Effective date: 2026-08-01

sha256:e33676bd0fd41f59162b6bec9d9d329b144547a10d34aadf1d57afda99cb271c

Dieses Dokument beschreibt etablierte Kontrollen. Es handelt sich weder um eine Zertifizierung noch um eine Garantie absoluter Sicherheit.

1. Governance und Zugang

Individueller Zugriff, RBAC, Rollenmanagement, Serverkontrollen, Überprüfung von Berechtigungen und Aufgabentrennung nach betrieblichen Erfordernissen.

2. Isolierung und Autorisierung

RLS, mandantenfähige Isolation, organisationsübergreifende Kontrollen, Zulassen von Player-Befehlen und serverseitige Verweigerung von Vorgängen außerhalb des Gültigkeitsbereichs.

3. Geheimnisse und Verschlüsselung

Auf der Serverseite gespeicherte Geheimnisse, keine Geheimnisse im Frontend, Verschlüsselung bei der Übertragung und verschlüsselte Speicherung entsprechend den Möglichkeiten des Anbieters. Für den Zugriff auf private Objekte werden bei Bedarf temporäre signierte URLs verwendet.

4. Protokollierung und Minimierung

Request_id, redigierte Protokolle, begrenzte Dauer, fehlende Eingabeaufforderungen in Analytics, Trennung von technischen Beweisen und Geschäftsinhalten.

5. Umgebungen und Tests

Trennung von Test und Produktion, synthetische Vorrichtungen, dedizierte Sandbox-Organisationen, Schutzmaßnahmen für echte Organisationen und das Fehlen organisationsübergreifender Mutationen in Tests.

6. Verfügbarkeit und Backups

Backups und Kontinuität entsprechend den Kapazitäten und technischen Zyklen der Lieferanten. Sicherungen werden nicht für geschäftliche Zwecke wiederverwendet und Löschungen werden bei Bedarf nach der Wiederherstellung erneut angewendet.

7. Vorfälle und Lieferanten

Vorfallverfahren, kontrollierte Beweissicherung, unverzügliche Benachrichtigung des Kunden, Tarifbegrenzung, Überwachung von Lieferanten und anwendbare vertragliche Übertragungsmechanismen.