Security & Compliance Overview

Security posture, certifications, and data-protection practices

Published: 2026-07-05 · **Classification:** Public · **Owner:** OptiSigns Security — security@optisigns.com

Statements are accurate as of the publication date and are regenerated from the canonical source on every posture-content release (annual review minimum).

Canonical, always-current version: https://www.optisigns.com/trust-center

Executive summary

OptiSigns is a cloud digital-signage platform serving **35,000+ customers and 200,000+ screens**. Organizations use OptiSigns to manage screens, content, and playback from a central web portal; the platform is operated from US cloud regions with EU/UK data-residency options.

This document is a point-in-time overview of our security posture for procurement, vendor-risk, and security-review teams: how customer data is protected (encryption, authentication, access control), how the platform is operated (network, device, and personnel security, vulnerability management, incident response, AI usage), and the independent attestations behind those statements. Each section is compiled verbatim from the same canonical source that powers our online Trust Center.

Deeper artifacts — audit reports, policies, test evidence — are listed in **Evidence available & how to request** at the end of this document.

Certifications & attestations at a glance

Attestation	Scope / status	Validity or as-of	How to obtain
SOC 2 Type 2 (Sensiba LLP)	Security, Availability, Confidentiality — unqualified opinion, no exceptions noted	Period ending 2025-11-15 (report 2025-12-22)	Under NDA via the security documentation request flow
TX-RAMP Level 1	Certified — Texas DIR Assessment path, Certificate ID TX1342625	Valid through 2028-07-31	Public record (Texas DIR certified-products list); certificate on request
HIPAA examination (AICPA attestation)	HHS HIPAA Audit Program — Security + Breach Notification Rules, zero exceptions (not intended for PHI; no BAAs)	As of 2025-11-15	Under NDA on request
GDPR DPA with EU SCCs + UK IDTA addendum	Art. 28 terms, authorized sub-processor list, 14-day change notice	Current revision 2026-04; UK addendum 2026-06	Public — optisigns.com/terms/dpa
Web-application penetration test	Annual, independent (most recent: Yappo Security, NIST SP 800-115, OWASP Top 10) — all findings remediated and validated	November 2025	Signed attestation letter on request

Certification and attestation details appear in the compliance sections at the end of this document.

Encryption at rest and in transit

Posture statement

All customer data is encrypted at rest and in transit. At rest, block storage on DigitalOcean is protected with 256-bit AES-XTS full-disk encryption, and objects in AWS S3 are encrypted with keys managed through AWS KMS. In transit, all traffic between players, browsers, and the OptiSigns cloud runs over HTTPS with TLS. The control "customer data at rest is encrypted" was tested in our most recent SOC 2 Type 2 examination with no exceptions noted.

How we implement

- **At rest — application and database tier.** Infrastructure hosted on DigitalOcean uses 256-bit AES-XTS full-disk encryption. Customer file uploads stored in AWS S3 are encrypted using AWS KMS-managed keys.
- **In transit.** All client-to-cloud and service-to-service communication uses HTTPS/TLS. Player devices connect outbound-only over TLS — see the “Network security and firewall whitelisting” section for the full port and endpoint list. TLS configuration on administrative tooling is covered by tested SOC 2 controls (CC6.6/CC6.7).
- **Credentials.** Customer authentication data is one-way encrypted (hashed) — passwords are never stored or transmitted in plaintext.
- **Backups.** All backups are encrypted and access to them is IAM-restricted. Backups run daily and are monitored.
- **Redundant object storage.** Every customer upload is stored in both AWS S3 and DigitalOcean Spaces — two independently encrypted cloud storage systems — removing any single-provider point of failure for customer content.
- **Workforce endpoints.** Hard-disk encryption is required and verified on employee workstations, so customer data handled internally stays encrypted at the endpoint as well.

We use industry-standard TLS 1.2+ in transit and AES-256 at rest; no FIPS 140-2/-3 validation is claimed. Key-management specifics beyond the above (e.g. rotation cadence) are documented internally and available on request via security@optisigns.com.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP; Security, Availability, Confidentiality) — available under NDA; includes the tested encryption controls with no exceptions noted.
- **Data Processing Addendum (DPA), Annex II** — our technical and organizational measures, including encryption of data at rest and in transit, published as part of our standard DPA.

- **Penetration-test attestation** (third-party, web application scope) — available on request; see the “Vulnerability management and penetration testing” section.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. Page validated 2026-07-02.

Related

- the “Network security and firewall whitelisting” section — TLS/443 outbound-only player traffic and firewall guidance
- the “Authentication — SSO, SAML, MFA, and passwords” section — how credentials and sessions are protected
- the “Incident response, breach notification, and resilience” section — encrypted backups in the resilience picture
- the “SOC 2 Type 2 attestation” section — the audit that tests these controls
- the “EU — GDPR compliance and data residency” section — encryption as a GDPR Art. 32 measure

Authentication — SSO, SAML, MFA, and passwords

Posture statement

OptiSigns supports enterprise authentication for customer accounts: SAML 2.0 single sign-on with the major identity providers, an enforced-SSO option that requires every user in the account to sign in through your IdP, and **native MFA — TOTP (authenticator app) and SMS** — for portal users. Internally, our workforce authenticates to cloud resources through Google Workspace SSO, with token-based (OTP) MFA required on sensitive systems.

How we implement

Customer-facing (product)

- **SAML 2.0 SSO** with Microsoft Entra ID (Azure AD), Okta, and Google Workspace. SAML SSO is available on Pro Plus and higher plans.
- **Enforced SSO.** Account admins can require that all users authenticate through the configured IdP. When SSO is enforced, your identity provider's own MFA and conditional-access policies govern every sign-in.
- **Native MFA for portal users** — TOTP (authenticator app) and SMS MFA are built into the portal and can be enabled per user; MFA is not forced on by default. Customers who need organization-wide mandatory MFA typically achieve it via enforced SSO through an IdP that requires it.
- **SCIM provisioning is not supported** — identity federation is SAML 2.0 SSO only. User management is handled in the OptiSigns portal.
- **Passwords** are one-way encrypted (hashed) and never stored or transmitted in plaintext. Password policy: **8–48 characters, requiring a lowercase letter, an uppercase letter, a number, and a symbol.** Under enforced SSO, your IdP's password policy governs.
- **Sessions** are persistent by default — there is no forced inactivity logout. Under enforced SSO, your identity provider's session policies apply.

Workforce (internal)

- **Google Workspace SSO** fronts our cloud resources; systems outside SSO use policy-conforming passwords.
- **Token-based (OTP) MFA** is required for cloud resources and sensitive systems — a tested SOC 2 control with no exceptions noted.
- **Remote administrative access** requires VPN with MFA; production server login is SSH-key-only.
- **Unique IDs** are required on the corporate network, production machines, network devices, and support tooling — no shared accounts.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; covers the tested workforce authentication and logical-access controls (no exceptions noted).
- **Product documentation** — SSO/SAML setup guides, MFA, and user-role articles are public in our support knowledge base.
- **InfoSec Policy summary** — available on request; the full policy is shared under NDA.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. Page validated 2026-07-02.

Related

- the “Access control — RBAC, folder permissions, and least privilege” section — what authenticated users can do (RBAC, folder permissions, teams)
- the “Employee access, screening, and offboarding” section — the full internal access-control picture
- the “Encryption at rest and in transit” section — how credentials and sessions are protected in transit and at rest
- the “SOC 2 Type 2 attestation” section — the audit covering these controls

Access control — RBAC, folder permissions, and least privilege

Posture statement

Access in OptiSigns is role-based at both layers. In the product, customers get role-based access control with user roles, folder-level permissions, and teams, so each user sees only the screens and content they should. Internally, access to production systems is provisioned on a least-privilege, as-needed basis and re-verified through quarterly access reviews of critical systems with an annual role-based review of access rules.

How we implement

Customer-facing (product)

- **Role-based access control (RBAC).** Assign users roles that scope what they can view and manage in the account.
- **Folder-level permissions.** Restrict content folders so users and teams only access the assets, playlists, and screens relevant to them.
- **Teams.** Segment larger organizations into teams with their own scoped content and screens.
- **Audit log.** Account activity can be captured in the audit log feature and queried/exported from the portal. The audit log is available on Pro Plus and higher plans; entries are retained for **2 years or 200,000 records, whichever comes first**, with longer retention available on request at additional cost.
- **SSO-based control.** With enforced SSO (see the “Authentication — SSO, SAML, MFA, and passwords” section), joiner/leaver control shifts to your IdP: disable the user there and they can no longer sign in.

Internal (workforce)

- **Least privilege.** Access is granted on an as-needed basis; new access needs are reviewed by management before being granted.
- **Recurring reviews.** We run quarterly access reviews of critical systems with an annual role-based review of access rules — tested SOC 2 controls with no exceptions noted.
- **Unique identities.** A unique ID is required for the corporate network, production machines, network devices, and support tools.
- **Hardened access paths.** Production server login is SSH-key-only; critical databases are IP-filtered so only authorized systems can reach them; remote administrative access requires VPN with MFA.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; includes the tested logical-access and access-review controls (no exceptions noted).

- **Product documentation** — user roles, folder-level permissions, teams, and audit-log articles are public in our support knowledge base.
- **InfoSec Policy summary** (including the Access Control sub-policy reference) — available on request.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. Page validated 2026-07-02.

Related

- the “Authentication — SSO, SAML, MFA, and passwords” section — how users prove who they are before RBAC applies
- the “Employee access, screening, and offboarding” section — workforce provisioning, reviews, and offboarding in detail
- the “Secure development lifecycle (SDLC)” section — change control on the systems these rules protect
- the “SOC 2 Type 2 attestation” section — the audit covering these controls

Employee access, screening, and offboarding

Posture statement

Internal access to systems that touch customer data is unique-identity, least-privilege, and MFA-protected, and it is re-verified through quarterly access reviews of critical systems with an annual role-based review of access rules. People controls run the full lifecycle: background checks at hire (as permitted by local law), mandatory annual security-awareness training, and a formal offboarding checklist with timely access revocation.

How we implement

Access

- **Workforce SSO + MFA.** Cloud resources sit behind Google Workspace SSO; token-based (OTP) MFA is required for sensitive systems; remote administrative access requires VPN with MFA.
- **Unique IDs, no shared accounts** — required across the corporate network, production machines, network devices, and support tools.
- **Least privilege.** Access is provisioned on an as-needed basis and new access needs are reviewed by management before grant.
- **Recurring reviews.** Quarterly access reviews of critical systems with an annual role-based review of access rules — tested SOC 2 controls, no exceptions noted.
- **Hardened paths.** Production server login is SSH-key-only; critical databases are IP-filtered.

People lifecycle

- **Hiring.** Background checks are performed for new hires as a condition of employment, as permitted by local law. At hire, employees acknowledge the InfoSec Policy, Code of Conduct, and Acceptable Use terms.
- **Training.** Security-awareness training is annual and mandatory for all full-time employees (tested, no exceptions noted).
- **Offboarding.** A formal termination checklist drives revocation of all access in a timely manner (tested control). We do not publish a fixed hour-count; the tested control is the commitment of record.
- **Reporting culture.** Everyone must report suspected security incidents immediately; a whistleblower policy with an anonymous reporting form protects reporters.

Endpoints and environment

- **Workstations** require hard-disk encryption; device policy adds screen-lock, antivirus, and restrictions on confidential data on mobile/USB media.

- **No owned physical facilities.** OptiSigns is 100% cloud and remote-first; physical security is inherited from the AWS and DigitalOcean data centers that host the service.
- **Governance.** The Information Security Policy (v3.0, 2025-10-27) — including a dedicated AI Acceptable Use section — is audited annually, alongside an annual company-wide risk assessment.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; covers the tested HR, logical-access, access-review, and offboarding controls (no exceptions noted).
- **InfoSec Policy summary** — available on request; the full policy is shared under NDA.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. InfoSec Policy v3.0 effective 2025-10-27. Page validated 2026-07-02.

Related

- the “Access control — RBAC, folder permissions, and least privilege” section — the shared least-privilege model, product and internal
- the “Authentication — SSO, SAML, MFA, and passwords” section — workforce SSO/MFA detail
- the “Incident response, breach notification, and resilience” section — where employee reports go
- the “Secure development lifecycle (SDLC)” section — engineering-specific controls
- the “SOC 2 Type 2 attestation” section — the audit covering these controls

Sub-processors

Posture statement

OptiSigns engages a defined list of sub-processors to deliver the service. The authorized list is part of our Data Processing Agreement (DPA §1(g), 2026-04 revision). Customers receive **14 days advance written notice** of sub-processor changes, with a right to object (DPA Attachment 1 / SCC Clause 9(a), general authorisation). All but two authorized sub-processors are located in the USA; the exceptions are Transloadit (Germany) and TypeForm (Spain).

Authorized sub-processors (the DPA list)

Vendor	Purpose	Location
Amazon (AWS)	Cloud hosting	USA
DigitalOcean	Cloud hosting	USA
MongoDB	Cloud database	USA
Google	Cloud storage / collaboration / marketing / analytics	USA
Cloudflare	Domain hosting / CDN	USA
Transloadit	File conversion	Germany
Zapier	Process automation	USA
Raintank (Grafana)	Log and monitoring	USA
Sentry.io	Log and monitoring	USA
HubSpot	CRM	USA
Customer.io	Customer communication	USA
Slack	Internal communication	USA
Zendesk	Issue management	USA
Stripe	Payments	USA
TypeForm	Customer survey	Spain
OpenAI	AI services	USA
Anthropic	AI services	USA
PostHog	Product analytics	USA

The list is periodically reconciled against our infrastructure; updates follow the DPA's 14-day notice.

Vendor management

OptiSigns maintains a vendor directory and performs an **annual review of critical-vendor compliance reports** under a formal Vendor Management Policy — a SOC 2-tested control with no exceptions noted (SOC 2 CC3.2/CC9.2).

Evidence available

The DPA, including the authorized sub-processor list and change-notice terms, is available to customers. SOC 2 Type 2 report (vendor-management controls) available under NDA.

Last review

Last audit: 2025-11-15 (SOC 2 period end). Page validated 2026-07-02.

Related

- the “AI usage and data handling” section — how the AI sub-processors are used and constrained
- the “Network security and firewall whitelisting” section — the endpoints these vendors operate
- the “EU — GDPR compliance and data residency” section — transfer mechanisms (EU SCCs, UK addendum) covering sub-processing

Network security and firewall whitelisting

Posture statement

All OptiSigns signage traffic is **outbound-only from the player over HTTPS on port 443**, with one legacy exception: a port-80 reachability check on Pro Players that is being confirmed/retired. Players never require inbound firewall rules, port-forwarding, or a VPN to operate. The recommended way to allow OptiSigns through a corporate firewall is by **FQDN (domain name), not by IP address** — the published IP addresses are load-balancer addresses and can change; domain-based rules stay correct as our infrastructure scales. The portal is fronted by Cloudflare's edge network; cloud infrastructure enforces deny-by-default inbound firewalling with NAT, and administrative access is restricted (SOC 2 §3).

How we implement

Whitelist by FQDN first

If your firewall supports wildcard domains, the simplest rule set is `.optisigns.com` + `.optisignsapp.com` on port 443. For granular allow-listing:

Purpose	Endpoint (FQDN preferred)	Port
Everything (wildcard)	*.optisigns.com*, .optisignsapp.com	443
API	api.optisigns.com · api.optisignsapp.com · api-prod-2/-3/-4.optisigns.com	443
WebSocket (realtime)	ws-prod-1/-2/-3.optisigns.com	443
MDM WebSocket	mdm-ws-prod-1/-2.optisigns.com	443
File/CDN	signagecloud-prd.nyc3.cdn.digitaloceanspaces.com · download.optisigns-cdn.com	443
Smallapps (weather/social/…)	smallapp.optisigns.com · smallapp-api.prod.optisignsapp.com	443
Pro Player OTA updates	software-update.optisigns.com · software-download.optisigns.com	443
Pairing	pairing.optisigns.com	443
Uploads (Transloadit)	*.transloadit.com*, .*.transloadit.com, s3.amazonaws.com, s3-eu-west-1.amazonaws.com	443
Designer images	plus.unsplash.com, images.unsplash.com	443
Remote control (RealVNC)	*.services.vnc.com	443
Short links (Bit.ly)	67.199.248.13, 67.199.248.12	443
AeriCast screen share	screenshare.aericast.com, present.aericast.com, apps-api-prd.aericast.com	443
Portal (browser access)	app.optisigns.com	443
Portal (legacy hostnames)	app1.optisigns.com · app3.optisigns.com · applive.optisigns.com	443

Signage traffic uses HTTPS/443, with one legacy exception: Pro Players perform a port-80 reachability check that is being confirmed/retired. If your egress policy is strictly 443-only, also allow outbound port 80 for Pro Players until that check is retired.

Fixed IPs (for IP-only firewalls / WAFs)

For gear that can only filter by IP — for example a WAF that must allow OptiSigns cloud to fetch a customer site for the Website app's screenshot path — four fixed addresses are published:

Fixed IP	Purpose
`157.230.201.46`	API
`206.189.255.219`	API
`52.217.39.148`	File delivery
`162.243.189.2`	File delivery

Prefer FQDNs wherever possible — the published IPs are load-balancer addresses and can change; FQDN-based rules are the complete, future-proof option.

What you do NOT need to whitelist

- **Website / web-scripting apps render on the player itself** — the player fetches the site directly; OptiSigns servers don't proxy it, so there is nothing inbound to whitelist (the fixed IPs above only matter when OptiSigns cloud must fetch your site, e.g. the screenshot path behind a WAF).
- **Social and Google apps have no fixed IP set** — those providers' CDNs rotate addresses; use domain rules.
- **CDN delivery can be disabled per account** on Engage/Enterprise plans if your network policy requires assets to come only from origin.

Per-device bandwidth consumption figures are not formally published — guidance for your deployment is available on request via security@optisigns.com.

Evidence available

SOC 2 Type 2 report (network architecture, firewalling, and monitoring controls) available under NDA. The player whitelist reference is published in our support knowledge base.

Last review

Last audit: 2025-11-15 (SOC 2 period end). Page validated 2026-07-02.

Related

- the “Device and player security” section — what runs on the players themselves
- the “Encryption at rest and in transit” section — TLS posture for the traffic described here
- the “Sub-processors” section — who operates the endpoints above

Vulnerability management and penetration testing

Posture statement

OptiSigns runs a recurring, audited vulnerability-management program: quarterly vulnerability scans with risk-ranked remediation, and an annual third-party penetration test of the web application. In the most recent penetration test (Yappo Security, November 2025), all findings were remediated by December 1, 2025 and the fixes were validated by the testing firm.

How we implement

- **Quarterly vulnerability scans.** Scans run on a quarterly cadence; identified issues are ranked by risk and remediated accordingly. This is a tested SOC 2 control (no exceptions noted).
- **Annual third-party penetration testing.** An independent firm performs a penetration test of the web application every year, with remediation tracked to closure under SLA-bound controls. The most recent engagement: **Yappo Security LLC**, web-application scope, November 3–10, 2025, following NIST SP 800-115 methodology with OWASP Top 10 and CWE/SANS Top 25 coverage. All findings were remediated by December 1, 2025 and validated by Yappo; a signed attestation letter (December 2, 2025) is available.
- **Risk assessment.** A formal risk assessment runs annually — threats are identified, ranked, and tracked against a managed remediation plan (tested, no exceptions noted).
- **Cloud-layer patching.** Infrastructure runs on managed AWS and DigitalOcean services, which handle platform-level patching; application-level fixes flow through our documented SDLC and release-approval process (see the “Secure development lifecycle (SDLC)” section).
- **Monitoring.** CPU/RAM/disk and service health are monitored across the fleet through automated monitoring and alerting on predefined rulesets, with on-call escalation.
- **Reporting a vulnerability.** Suspected security issues can be reported to **security@optisigns.com** and are triaged through our incident-response process — see the “Vulnerability disclosure policy” section for our disclosure policy and the “Incident response, breach notification, and resilience” section for what happens next.

Evidence available

- **Penetration-test attestation letter** (Yappo Security LLC, signed 2025-12-02) — a summary attestation built to share with customers; the full findings report is an internal artifact.
- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; covers the tested vulnerability-scanning, remediation, and risk-assessment controls (no exceptions noted).

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. Pen-test attestation signed 2025-12-02. Page validated 2026-07-02.

Related

- the “Vulnerability disclosure policy” section — how to report a vulnerability to us
- the “Secure development lifecycle (SDLC)” section — how fixes ship (SDLC, testing, release approval)
- the “Incident response, breach notification, and resilience” section — what happens when an issue becomes an incident
- the “Network security and firewall whitelisting” section — the network surface these tests probe
- the “SOC 2 Type 2 attestation” section — the audit covering these controls

Incident response, breach notification, and resilience

Posture statement

OptiSigns maintains a documented Incident Response Plan with defined roles and procedures, tested annually. Incidents are logged, classified, and tracked to resolution with lessons learned. If a personal data breach affects a customer, we notify the customer in writing **without undue delay** upon becoming aware of it, per our Data Processing Addendum and consistent with GDPR.

How we implement

Incident response

- **Documented IR Plan.** Roles, responsibilities, and procedures are defined in a formal Incident Response Plan, exercised at least annually — a tested SOC 2 control with no exceptions noted.
- **Formal incident handling.** Incidents are logged, classified by severity, escalated, and tracked to resolution, with post-incident lessons learned feeding back into controls.
- **Everyone reports.** All personnel must report suspected security incidents immediately. A whistleblower policy with an anonymous reporting channel backs this up (see the “Employee access, screening, and offboarding” section).
- **Breach notification.** The commitment in our standard DPA is notification **without undue delay** after we become aware of a personal data breach affecting customer personal data — consistent with GDPR, whose Art. 33 sets a 72-hour supervisory-notification backstop — with the information customers need for their own regulatory obligations. The contractual wording is the commitment of record.

Resilience (DR / BC / backups)

- **Disaster Recovery and Business Continuity Plans** are documented and tested annually (tested SOC 2 controls, no exceptions noted).
- **Recovery objectives.** Our recovery objectives are an **RTO of 4 hours and an RPO of 4 hours** (in practice, as a non-transactional system, data loss exposure is typically near zero; all tested DR scenarios recovered in under 2 hours). These are operational targets; our contractual availability commitment is the uptime SLA below.
- **Uptime SLA.** OptiSigns commits to a **99.99% monthly uptime SLA**, published at optisigns.com/terms/sla, with service credits for misses.
- **Backups** are automated, encrypted, monitored, and IAM-restricted, with **point-in-time restore**; tiered snapshots are retained up to 2 months on the primary database. Backups are stored offsite across dual, independent cloud providers.
- **No single point of failure.** The application tier auto-scales on Kubernetes, databases are replicated, and every customer upload is stored in **both AWS S3 and DigitalOcean Spaces** — dual, independent object

stores.

- **Capacity monitoring** covers compute, memory, and disk across the fleet with alerting on predefined rulesets.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; covers the tested incident-response, backup, and BC/DR controls (no exceptions noted), and notes no significant incidents during the audit period.
- **Data Processing Addendum (DPA)** — the breach-notification commitment, published as part of our standard terms.
- **InfoSec Policy summary** (Incident Response Plan and BC & DR Plan sub-policy references) — available on request.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. Page validated 2026-07-02.

Related

- the “Vulnerability management and penetration testing” section — finding issues before they become incidents
- the “Encryption at rest and in transit” section — encrypted backups and dual-cloud storage detail
- the “Employee access, screening, and offboarding” section — reporting duties and the anonymous channel
- the “SOC 2 Type 2 attestation” section — the audit covering these controls
- the “EU — GDPR compliance and data residency” section — the regulatory frame for breach notification

AI usage and data handling

Posture statement

OptiSigns uses AI in two customer-facing features — the **AI Designer** (content generation inside the design tool) and the **OptiBot support chatbot** — plus internal agent tooling for support and sales operations. **OptiSigns does not train models on customer data, and customer content sent to AI features is not used to train models** — a stance that applies to the DPA-authorized AI providers. The authorized AI sub-processors in our Data Processing Agreement (2026-04 revision) are **OpenAI and Anthropic (both USA)**. Under the EU AI Act we self-classify our AI features as **limited/minimal risk**.

How we implement

AI providers and contracts

- **OpenAI and Anthropic** are the AI sub-processors authorized in the DPA (2026-04 revision); see the “Sub-processors” section for the full sub-processor list and change-notice terms.
- **No-training stance:** customer content sent to AI features is used only to produce the requested output — it is not used to train models. This stance is scoped to the DPA-authorized AI providers (OpenAI and Anthropic).
- AI data handling is governed by our Data Processing Agreement; sub-processor changes follow the DPA's 14-day-notice terms.

Logging and retention

- Prompt logs are retained for a limited period for security and abuse monitoring; they are never exposed to other customers. Current retention specifics are available on request via security@optisigns.com.

Internal AI acceptable use

Our Information Security Policy (v3.0, October 2025, §8) sets a formal AI Acceptable Use policy for the workforce:

- Company-**approved AI tools only**; no confidential or customer data may be entered into unapproved AI systems.
- **Human review of AI output** before it is used or deployed.
- AI-generated code goes through the same **secure SDLC** (review, testing, approval) as any other code.
- **No business-critical decision is made by AI alone.**
- The company may monitor and restrict AI tool usage.

AI camera add-on (product)

The optional AI camera add-on performs facial **detection, not facial recognition**. It produces **anonymous counts only** (person/face, gender, age band), the analysis is **processed locally on the device**, and **no images or facial identifiers are stored** on OptiSigns servers or on the device — unless the customer explicitly enables image storage, in which case the customer owns compliance for that stored imagery.

Regulatory classification

- **EU AI Act:** self-classified as limited/minimal risk.
- AI features are covered by the same GDPR Art. 28 DPA terms as the rest of the platform — see the “EU — GDPR compliance and data residency” section.

Evidence available

DPA (including the authorized sub-processor list) available to customers; Information Security Policy summary available on request; SOC 2 Type 2 report under NDA.

Last review

Last audit: 2025-11-15 (SOC 2 period end). Page validated 2026-07-05 (§8 cite re-verified against the v3.0 master PDF).

Related

- the “Sub-processors” section — authorized sub-processors, including AI providers
- the “Device and player security” section — the AI camera's on-device processing model
- the “EU — GDPR compliance and data residency” section — DPA structure and transfer mechanisms

Secure development lifecycle (SDLC)

Posture statement

OptiSigns ships software through a documented Secure Development Lifecycle: every change is version-controlled, tested in pre-production environments, and approved before it reaches production. These change-management controls were tested in our most recent SOC 2 Type 2 examination with no exceptions noted, and the annual third-party penetration test of the web application validates the result from the outside.

How we implement

- **Documented SDLC policy.** Secure development is a formal sub-policy of the Information Security Policy, and change management is a tested SOC 2 control area (CC8.1, no exceptions noted).
- **Version control everywhere.** All source code lives in GitHub and GitLab with tracked history, so every production change is attributable and reviewable.
- **Pre-production testing.** Changes are tested in non-production environments before release; work is managed through an Agile backlog with defined acceptance.
- **Release approval.** Releases require approval before deployment to production — no direct, unreviewed pushes to the live service.
- **Separation of duties.** Access to production deployment paths follows the least-privilege and unique-ID controls described in the “Access control — RBAC, folder permissions, and least privilege” section.
- **Security feedback loops.** Quarterly vulnerability scans and the annual third-party penetration test of the web application (see the “Vulnerability management and penetration testing” section) feed findings back into the backlog with risk-ranked remediation; the annual risk assessment covers development-process threats as well.
- **AI-assisted development, governed.** The InfoSec Policy v3.0 (2025-10-27) includes a formal AI Acceptable Use section: only company-approved AI tools may be used, no confidential or customer data goes into unapproved AI systems, AI output is human-reviewed before use or deployment, and AI-generated code follows the same secure SDLC as human-written code.
- **Engineers are trained.** All full-time employees, including engineering, complete mandatory annual security-awareness training.

Specific tooling names and internal pipeline details are deliberately not published here; additional detail for security reviews is available on request via security@optisigns.com.

Evidence available

- **SOC 2 Type 2 report** (Sensiba LLP) — available under NDA; covers the tested SDLC/change-management controls (version control, pre-production testing, release approval) with no exceptions noted.

- **Penetration-test attestation** (third-party, web-application scope; most recent: Yappo Security, November 2025, all findings remediated and validated December 2025) — available on request.
- **InfoSec Policy summary** (Secure Development and AI Acceptable Use sections) — available on request.

Last review

SOC 2 Type 2 period ending 2025-11-15, report dated 2025-12-22. InfoSec Policy v3.0 effective 2025-10-27. Page validated 2026-07-02.

Related

- the “Vulnerability management and penetration testing” section — scans and pen tests that validate the SDLC output
- the “Employee access, screening, and offboarding” section — the people controls behind the process
- the “Access control — RBAC, folder permissions, and least privilege” section — least privilege on production deployment paths
- the “SOC 2 Type 2 attestation” section — the audit covering these controls

Device and player security

Posture statement

OptiSigns first-party devices (OptiStick, Pro Player) are **purpose-built signage players running OptiSigns-signed software** — not generic consumer TV boxes. The OptiStick ships with Android verified boot and file-based encryption; the Pro Player (Intel) ships with TPM2-backed full-disk encryption and a sealed read-only OS. First-party devices receive automatic signed updates and communicate **outbound-only over TLS** (see the “Network security and firewall whitelisting” section for ports and endpoints). On bring-your-own-device platforms (customer-supplied Android, Fire TV, Windows/Mac via Electron, or the browser WebPlayer), the OptiSigns player is an application and device-level security inherits the host operating system.

How we implement

Firmware supply-chain trust

Customers sometimes ask whether inexpensive Android sticks are safe in light of supply-chain malware campaigns such as Badbox 2.0, which targeted generic AOSP TV boxes. The OptiStick is not a generic AOSP TV box: it runs the OptiSigns player as a **signed system app** on a device with a **locked bootloader and Android verified boot** (verifiedbootstate green), **file-based encryption**, and approximately quarterly vendor security ROM OTAs. The Pro Player (Intel) runs OptiSigns' own hardened Linux with **TPM2-backed LUKS full-disk encryption**, a **sealed read-only root filesystem**, and **A/B over-the-air updates with automatic rollback** if an update fails; remote shell access in production is gated behind the SecureLink (WireGuard) VPN. Player software self-updates automatically through OptiSigns-controlled channels.

Per-family posture

Device family	Storage encryption	Boot / OS integrity	Updates	Kiosk lockdown
OptiStick (first-party)	Android file-based encryption	Locked bootloader + Android verified boot (green)	App self-update + ~quarterly vendor security ROM OTAs	Yes
Pro Player (Intel, first-party)	TPM2-backed LUKS full-disk encryption	OptiSigns-hardened Linux, sealed read-only root filesystem	A/B OTA with rollback + app self-update	Yes
BYOD Android	Inherits host OS (Android 10+ defaults to file-based encryption)	Varies by OEM	Player self-update (user-approved) + OEM OTAs	Requires Device Owner enrollment
Fire TV	Inherits Fire OS (file-based encryption, Amazon locked bootloader)	Amazon-managed	Player self-update + Amazon Fire OS OTAs	No
Electron (Win/Mac/Linux)	Host-managed (BitLocker / FileVault / LUKS)	Host-managed	Player auto-update	No
WebPlayer (browser)	n/a — browser sandbox	n/a	Always fresh from CDN	n/a

Additional device controls

- **Enterprise Wi-Fi (802.1X EAP, certificate-based)** is supported on OptiStick and Pro Player.
- **Wi-Fi security:** player Wi-Fi code supports WPA2 and WPA3; per-model support can be confirmed with our engineering team during security review.
- **Wi-Fi credentials on the OptiStick are stored encrypted**; OptiSigns staff cannot view them. Files stored on the OptiStick are encrypted at rest.
- **Content preconfiguration** uses an encrypted boot configuration file (AES-encrypted).
- **OptiSigns SecureLink** (WireGuard VPN) is available on OptiStick and Pro Player for authorized remote-support access — outbound-initiated, no inbound firewall holes.
- **Kiosk/lockdown mode** on first-party devices prevents users from leaving the signage experience; on BYOD Android it requires Device Owner enrollment.

Evidence available

SOC 2 Type 2 report available under NDA. Device capability specifics (per-model encryption and boot posture) can be confirmed with our engineering team during security review.

Last review

Last audit: 2025-11-15 (SOC 2 period end). Page validated 2026-07-02.

Related

- the “Network security and firewall whitelisting” section — what the devices talk to and how to whitelist it
- the “Encryption at rest and in transit” section — platform-wide encryption posture
- the “Sub-processors” section — third parties involved in device services (e.g. remote access)

Vulnerability disclosure policy

Posture statement

OptiSigns welcomes good-faith security research. If you believe you have found a vulnerability in an OptiSigns product or service, report it to **security@optisigns.com** and we will work with you to understand, validate, and remediate the issue. We do not currently operate a paid bug-bounty program.

How to report

- Email **security@optisigns.com** with a description of the issue, the steps to reproduce it, and the potential impact. Include screenshots, request/response samples, or proof-of-concept detail where it helps.
- We will **acknowledge your report within 5 business days** and keep you informed as we validate and remediate.
- Please give us reasonable time to remediate before any public disclosure.

Scope

- The OptiSigns web portal (**app.optisigns.com**) and related web properties
- OptiSigns **player applications and first-party devices** (OptiStick, Pro Player, Android, Fire TV, Electron, WebPlayer)
- OptiSigns **APIs** (REST and GraphQL)

Good-faith research (safe harbor)

We will not pursue legal action against researchers who report vulnerabilities in good faith and follow this policy:

- **Do not access, modify, or delete data that is not yours.** If a proof of concept would touch another customer's data, stop and report what you have.
- **Do not degrade the service** — no denial-of-service testing, spam, or social engineering of OptiSigns staff or customers.
- **Give us reasonable time to remediate** before sharing details publicly.
- Only test against accounts you own or are authorized to use.

Reports made in line with the above are considered authorized good-faith research; we will not initiate legal action for them.

security.txt

The canonical machine-readable disclosure record for OptiSigns (RFC 9116 `security.txt`) carries:

```
Contact: mailto:security@optisigns.com
Policy: https://trust.optisigns.com/vulnerability-disclosure
```

Last review

Page validated 2026-07-02.

Related

- the “Vulnerability management and penetration testing” section — our internal scanning, pen-test, and remediation program
- the “Incident response, breach notification, and resilience” section — how confirmed issues are handled
- the “Network security and firewall whitelisting” section — the network surface in scope

SOC 2 Type 2 attestation

OptiSigns maintains a **SOC 2 Type 2** attestation — an independent, period-of-time examination of our security program, not a point-in-time snapshot.

Current report

Item	Value
Report type	SOC 2 **Type 2**
Independent auditor	**Sensiba LLP** (San Jose, CA)
Report date	**2025-12-22**
Audit period	**November 16, 2024 → November 15, 2025**
Trust services criteria in scope	**Security, Availability, Confidentiality**
Opinion	**Unqualified (clean)** — no exceptions noted in the tests of controls
Incidents	No significant incidents during the audit period
Track record	3+ consecutive annual SOC 2 Type 2 periods

The audit is annual; each new period picks up where the prior one ends, so coverage is continuous year over year.

How to get the report

The full report is shared **on request via the security documentation request flow**: an expiring tokenized download link with a one-line click-through confidentiality acknowledgment — no NDA wall. Requesters who need an explicit NDA are accommodated on request. Always share the **current** report (check the period end date on the artifact before forwarding anything).

A standing **bridge letter** covering November 16, 2025 → November 15, 2026 is issued per-customer on request. It is an exception path for requesters who explicitly need gap coverage between the report date and their review date — most requests are fully satisfied by the current report itself.

What OptiSigns is — and is not — certified for

Say these honestly and exactly:

- **ISO 27001:** OptiSigns is not ISO 27001 certified — we maintain a SOC 2 Type 2 attestation; our underlying cloud providers (AWS, DigitalOcean, MongoDB Atlas, Cloudflare) hold ISO 27001.
- **FedRAMP:** OptiSigns is **not FedRAMP authorized**. We hold **TX-RAMP Level 1** instead — see the "TX-RAMP Level 1 certification" section. For federal requirements, offer the SOC 2 + pen-test + DPA package.

- **HITRUST:** not held.
- **PCI-DSS:** OptiSigns is **not PCI-DSS-certified** and does not need to be for payments — **Stripe processes all payment card data; we never store card numbers**.
- **CMMC:** not held.

Answering the common asks

- *"Are you SOC 2 certified?"* — Yes: SOC 2 **Type 2**, clean unqualified opinion, no exceptions noted, audited annually by Sensiba LLP.
- *"Which trust criteria are in scope?"* — Security, Availability, and Confidentiality.
- *"Can we see the report?"* — Yes: request it via the security docs request flow and you receive an expiring tokenized download link with a one-line confidentiality acknowledgment; an explicit NDA is accommodated on request.
- *"Is the current-year report available?"* — Yes. The report dated 2025-12-22 covering the period ending November 15, 2025 is final and available now.

For operational numbers (uptime SLA, backup/recovery objectives, retention windows), see the relevant security posture pages.

TX-RAMP Level 1 certification

OptiSigns holds a **TX-RAMP Level 1 certification**, the Texas Risk and Authorization Management Program administered by the Texas Department of Information Resources. TX-RAMP certification is what Texas state agencies (and many Texas public institutions that follow DIR guidance) require before adopting a cloud service.

Status

Item	Value
Program	TX-RAMP (Texas Risk and Authorization Management Program)
Level	**Level 1**
Status	**Certified** — Certificate ID **TX1342625**, granted **2025-08-01**, valid through **2028-07-31** (DIR Assessment path; listed on the Texas DIR public certified-products list)
History	Provisional certification first granted in 2023
Framework basis	**NIST 800-53**-based control program

TX-RAMP assessments are built on the NIST 800-53 control catalog, so a TX-RAMP certification signals that OptiSigns' security program has been evaluated against the same control family that underpins US government cloud-security frameworks.

TX-RAMP vs FedRAMP

These are different programs, and we state the difference plainly:

- **OptiSigns is not FedRAMP authorized**, and does not claim or imply otherwise.
- **OptiSigns holds TX-RAMP Level 1.** That satisfies Texas state-agency requirements; it is not a federal authorization.
- For **federal buyers whose process requires FedRAMP**: we offer our **SOC 2 Type 2 report + third-party pen-test attestation + DPA** as the evidence package (the “SOC 2 Type 2 attestation” section). Many federal-adjacent and prime-contractor reviews accept that package for a signage workload.

Answering the common asks

- *"Are you FedRAMP authorized?"* — No. We hold **TX-RAMP Level 1** (NIST 800-53-based; Certificate ID TX1342625, valid through 2028-07-31), and we can provide the SOC 2 Type 2 + pen-test + DPA package for federal security reviews.
- *"Are you approved for Texas state agencies?"* — Yes: TX-RAMP Level 1.

- *"Can we see the certificate?"* — Yes, via the security documentation request flow.
- *"What level is your TX-RAMP?"* — Level 1, which covers non-confidential and public data categories as defined by DIR; agencies map their own data classification to the required level.

Related posture

- SOC 2 Type 2 attestation (the anchor artifact for most security reviews) — the “SOC 2 Type 2 attestation” section
- US hosting and data residency for government buyers — the “US — hosting and data residency” section

HIPAA examination — Security and Breach Notification Rules

OptiSigns is not intended for PHI. Digital signage content is public display content — healthcare customers use OptiSigns for waiting-room information, wayfinding, menus, and announcements, never patient-identifying information. We are not a covered entity, and we do not sign Business Associate Agreements.

Even so, healthcare organizations vet every vendor's safeguards. So we had ours independently examined: an AICPA attestation examination against the **HHS HIPAA Audit Program (July 2018) — Security Rule and Breach Notification Rule protocols** — with **zero exceptions**, as of **November 15, 2025**.

Status

Item	Value
Examination	AICPA attestation examination of management's assertion
Standard	HHS **HIPAA Audit Program (Updated July 2018)** — Security Rule + Breach Notification Rule protocols
Result	**Clean opinion — zero exceptions** across all tested protocol items
As of	**2025-11-15** (report issued 2025-12-22, same auditor and period end as our SOC 2 Type 2)
Privacy Rule	Not applicable — OptiSigns is not a covered entity (stated in the examination)

What we claim — precisely

- **We do not claim "HIPAA certified" or "HIPAA compliant."** No such certification exists, and HIPAA compliance obligations attach to entities that handle PHI — which the platform is not intended to do. What we claim, precisely: our safeguards were **independently examined against the HHS HIPAA Audit Program with zero exceptions**.
- **We do not sign BAAs.** Because no PHI should ever be placed on the platform, a Business Associate relationship does not arise. Customers must not put PHI on screens.
- **Why it still matters:** hospital and health-system vendor-risk reviews assess safeguards against HIPAA Security Rule line items regardless of PHI exposure. This examination lets those reviews check that box with independent evidence instead of vendor self-attestation.

Answering the common asks

- *"Are you HIPAA compliant?"* — OptiSigns is not intended for PHI and does not sign BAAs; HIPAA compliance obligations therefore do not attach. Our safeguards have been independently examined

against the HHS HIPAA Audit Program (Security + Breach Notification Rules) with zero exceptions, as of 2025-11-15.

- *"Will you sign a BAA?"* — No. The platform is not designed for PHI workloads and our data-processing terms anticipate no sensitive data.
- *"Can we see the examination report?"* — Yes, under NDA via the security documentation request flow (same handling as our SOC 2 report).
- *"How do you notify us of a breach?"* — Per our DPA: without undue delay upon becoming aware — see the “Incident response, breach notification, and resilience” section.

Related posture

- SOC 2 Type 2 attestation (same auditor and period end) — the “SOC 2 Type 2 attestation” section
- Incident response and breach notification — the “Incident response, breach notification, and resilience” section
- Privacy posture and DPA structure — the “EU — GDPR compliance and data residency” section

US — hosting and data residency

OptiSigns is **hosted in the United States by default**. This page is the canonical answer to "where is our data?" for US customers and for anyone who hasn't purchased regional residency.

Where the data lives

Layer	Provider / location
Application + managed services	**DigitalOcean (NYC)**
Object storage + CDN + email	**AWS (N. Virginia)**
Primary application database	**MongoDB Atlas** (AWS us-east-1)
Edge / DNS / routing	**Cloudflare** (global edge; origin data stays US)

A notable, audit-backed redundancy property: **dual object storage** — every customer upload is stored in **both AWS S3 and DigitalOcean Spaces**, two independent cloud providers.

Physical security — 100% cloud

OptiSigns owns **no data centers**; the platform is 100% cloud-hosted. Physical security is **inherited from the cloud providers'** audited data-center controls, and that inheritance is covered in our **SOC 2 Type 2** report (the “SOC 2 Type 2 attestation” section). The underlying providers (AWS, DigitalOcean, MongoDB Atlas, Cloudflare) hold ISO 27001; OptiSigns itself maintains the SOC 2 Type 2 attestation.

State and local government

For Texas state agencies and DIR-aligned public institutions, OptiSigns holds **TX-RAMP Level 1** — see the “TX-RAMP Level 1 certification” section. For other state/local reviews, the SOC 2 Type 2 + pen-test + DPA package is the standard evidence set.

Residency boundaries

- **Regions offered:** US default (AWS N. Virginia + DigitalOcean NYC + MongoDB Atlas us-east-1), with EU (Frankfurt/Amsterdam) and UK (London) residency available on the Engage plan (the “EU — GDPR compliance and data residency” section). No other regional residency (including Australia) is offered.
- **Provider and region are not customer-selectable** beyond the Engage EU/UK option above.
- **No owned facilities.** OptiSigns runs entirely on major cloud providers; physical security is inherited from their audited data-center controls.

Answering the common asks

- *"Where is our data hosted?"* — In the United States: AWS (N. Virginia) and DigitalOcean (NYC), with MongoDB Atlas as the primary database and Cloudflare at the edge.
- *"Is our content backed up across providers?"* — Every upload is stored in both AWS S3 and DigitalOcean Spaces — two independent clouds.
- *"Can we get data residency in Australia?"* — No. Residency options are US (default) and EU/UK on the Engage plan.
- *"Who handles physical security?"* — The cloud providers; OptiSigns is 100% cloud with no owned data centers, and the inheritance is covered in our SOC 2 Type 2 report.

EU — GDPR compliance and data residency

OptiSigns is **GDPR-compliant**. We do not claim to be "GDPR certified" — **no GDPR certification exists**; the substance is the DPA, the SCCs, and the controls behind them.

The DPA (public)

Our Controller → Processor **Data Processing Agreement with GDPR Art. 28 terms** is publicly available at **optisigns.com/terms/dpa**. Key terms:

- **EU transfers:** the **EU Standard Contractual Clauses (2021/914), Module Two (Controller-to-Processor)** are attached as **DPA Attachment 1**; governing law **Ireland**.
- **UK transfers:** the **UK ICO IDTA Addendum (v B1.0)** is available (added 2026-06) and is appended to the DPA for UK customers.
- **TOMs:** technical and organisational measures are documented in **DPA Annex II**.
- **Sub-processors:** the authorized list is maintained at the “Sub-processors” section, with **14-day advance written notice** of changes and a **right to object**.
- **Breach notification:** we notify **"without undue delay"** on becoming aware of a personal data breach, consistent with GDPR (the 72-hour supervisory-notification backstop of GDPR Art. 33 applies). The contractual wording is the commitment of record.
- **DSR + assessment assistance:** we assist with data-subject requests and with GDPR **Arts. 32–36** obligations (security, breach, DPIA, prior consultation), at customer cost.
- **Customer audits:** information on request, plus a maximum of **1 customer audit per 12 months**.
- **Sensitive data:** the parties do not anticipate the transfer of sensitive data (DPA Annex I.B).

DPO / privacy contact: **Frank Gao, Head of Information Security** (per DPA Annex I.A).

Data residency

- **Default: United States** — AWS (N. Virginia) + DigitalOcean (NYC) + MongoDB Atlas (us-east-1).
- **EU residency (Frankfurt/Amsterdam) and UK residency (London) are available on the Engage plan.** Once enabled, **new uploads go to the EU/UK region; pre-existing content stays where it is unless re-uploaded**.
- No other regions are currently offered.

Honest statements — international transfers

- **OptiSigns does not participate in the EU-US Data Privacy Framework; EU transfers rely on Standard Contractual Clauses (per our DPA)** — plus the UK addendum for UK transfers. This is a complete, lawful transfer mechanism.

- EU-representative arrangements: contact **security@optisigns.com** for current details.

Customer rights, self-serve

Users can **download and delete their data self-serve** in the platform, and a **published deletion-request process** covers the rest — useful concrete answers for Art. 15/17 questions.

Answering the common asks

- *"Are you GDPR certified?"* — No such certification exists. We are GDPR-compliant: public DPA with Art. 28 terms, EU SCCs Module Two, UK IDTA addendum, documented TOMs, and a maintained sub-processor list with 14-day change notice.
- *"Can our data stay in the EU?"* — Yes, on the Engage plan (Frankfurt/Amsterdam; London for UK); new uploads land in-region, pre-existing content stays unless re-uploaded.
- *"How fast do you notify on a breach?"* — Without undue delay, consistent with GDPR (72-hour supervisory-notification backstop, GDPR Art. 33).
- *"Are you DPF certified?"* — OptiSigns does not participate in the EU-US Data Privacy Framework; EU transfers rely on Standard Contractual Clauses (per our DPA).

Evidence available & how to request

Our security documentation is tiered by sensitivity:

- **Public** — this document, the online Trust Center (www.optisigns.com/trust-center), our DPA (optisigns.com/terms/dpa), and security.txt.
- **On request** — our completed CSA CAIQ-Lite v4 self-assessment (spreadsheet + PDF), information-security policy summaries, the platform architecture diagram, the signed penetration-test attestation letter, VPAT (with currency caveat), certificate of insurance.
- **Under NDA** — SOC 2 Type 2 report and HIPAA examination report, via an expiring tokenized link with a confidentiality acknowledgment.

To request any artifact — or to report a security issue — contact **security@optisigns.com**. Completed security questionnaires are handled through the same channel.