

Screenzor

Security Statement

Last revised: August 17, 2026

This page describes, in plain language, how we protect your data. It is not a substitute for our Privacy Policy (<https://screenzor.com/privacy-policy>), which governs what data we collect and why.

1. Infrastructure

Screenzor is built on established infrastructure providers — Supabase for authentication, database, and file storage, and a major cloud hosting provider (AWS/GCP/Azure/Cloudflare) — rather than self-managed servers. We rely on these providers' own security certifications and practices as part of our overall security posture; details on our current sub-processors are listed in our Privacy Policy (<https://screenzor.com/privacy-policy>).

2. Encryption

Data is encrypted in transit (HTTPS/TLS) between your browser or the Screenzor extension and our servers. Data at rest (account data, uploaded recordings, and Google Calendar integration data when connected) is encrypted using our infrastructure providers' storage-level encryption. Google Calendar refresh tokens are additionally encrypted with AES-256-GCM before they are stored. Google Calendar OAuth uses PKCE (S256).

3. Access Controls

Access to Customer Personal Data within Screenzor's systems is limited to what is necessary to operate and support the Service. Users must be signed in to access their own account and Calendar data. Calendar API routes that read or change a user's Calendar data require a valid authentication token for the signed-in user. Database row-level security restricts Calendar and account rows so that an authenticated user can access only their own data. Google Calendar refresh tokens are encrypted before they are stored and are not returned by Screenzor's Calendar APIs.

As a small, single-operator business, the operator may access hosted infrastructure (including the database) as needed to operate, maintain, and support the Service. Screenzor does not currently use a separate enterprise role-based access-control system or a formal admin audit log for this data.

4. Local vs. Uploaded Recordings

As described in our Extension Permissions Disclosure (<https://screenzor.com/extension-permissions-disclosure>), recordings you make without uploading never reach Screenzor's servers. Only recordings you choose to upload (e.g. to generate a shareable link or use team workspace features) are transmitted to and stored on our infrastructure.

5. Breach Notification

If a data breach occurs that is likely to result in risk to your rights, we will notify affected users and, where required, the relevant regulator, consistent with Section 10 of our Privacy Policy (<https://screenzor.com/privacy-policy>).

6. Reporting a Security Issue

If you are a security researcher and believe you've found a vulnerability, see our Vulnerability Disclosure Policy (<https://screenzor.com/vulnerability-disclosure-policy>) for how to report it safely. For any other security question, contact legal@screenzor.com.

7. What We Don't Yet Have

As a small, single-operator business, we do not currently hold formal third-party security certifications (e.g. SOC 2, ISO 27001). This section will be updated if and when that changes.

8. Changes to This Statement

See the notice at the end of this document for how we handle changes to this statement.

Last revised: August 17, 2026

We may update this document from time to time. If we make material changes, we will notify you by email and/or a notice on the Screenzor website before the change takes effect. Minor changes will only update the date above.