PhotoSentinel
A story in every frame.

Security Overview

Version 1.0 · Issued 21 August 2026
Public

Your site imagery is a record of how something got built. Sometimes it's the only record. We treat it that way. This document sets out what protects your data, what we hold, and what we don't. It's written to be checked.

ACCESS AND AUTHENTICATION

Only authenticated users with valid credentials can access or configure a system in Sentinel OS. Stored passwords are salted and hashed. Access is role based, so an administrator can give a client imagery from selected cameras without the ability to change a single system setting.

Customer sign-in runs through Clerk. Our own staff reach company systems through Microsoft Entra with single sign-on and conditional access, and reaching the production database additionally requires our VPN.

ENCRYPTION

At rest, your content is encrypted with AES-256 across both of our storage providers. Account credentials carry a further layer of application-level encryption on top of that.

Imagery is delivered from our platform to your browser over HTTPS.

The upload path from the camera depends on the unit installed on your site. We state it exactly, for your fleet, in the statement described below.

CONTROLLED IMAGE ACCESS

By default your imagery is available only to authenticated users over HTTPS. When you choose to share an image, we generate a time-limited signed link.

Sharing is a decision you make, not a default we set.

WHERE YOUR DATA GOES

Different customers carry different obligations. Rather than publish one answer that fits nobody, we'll give you a written Statement of Data Processing, Flows and Jurisdictions for your deployment: where your imagery is transferred, processed and stored, which companies hold it, what protects it, and which laws reach it. Ask your account manager and we'll issue it.

For customers with in-country requirements in Saudi Arabia, we operate a data-sovereign environment in Jeddah on Oracle infrastructure, with its own compute and storage.

WHEN YOU SEND IMAGERY SOMEWHERE ELSE

Sentinel OS can forward your imagery to systems you nominate, including Procore, Dropbox, OneDrive, Google Drive, and your own FTP or cloud storage. When you switch that on, imagery goes where you've asked us to send it and is held under that provider's terms rather than ours.

We'll list every destination configured for you in your statement, so your obligations are assessed against what actually happens rather than what we hold.

YOUR IMAGERY IS YOURS

The imagery your cameras capture belongs to you. We retain only anonymised system telemetry about how the equipment is performing. The wording in your contract prevails over this summary.

WHAT WE HOLD, AND WHAT WE DON'T

We're working toward ISO/IEC 27001 certification through a formal programme, with an external auditor engaged. We're not certified today, and we'll say so until we are.

We hold no IRAP assessment, no Hosting Certification Framework certification, and no DISP membership. If your project requires any of those, tell us early and we'll tell you honestly whether we can serve it.

REPORTING A SECURITY ISSUE

If you believe you've found a vulnerability, email support@photosentinel.com and it will reach our team.

DOCUMENT	**PhotoSentinel Pty Ltd — Security Overview**
VERSION	**1.0 · issued 21 August 2026**
CLASSIFICATION	**Public**
CONTACT	**support@photosentinel.com**
GENERATED	**16 October 2026**