INVIGILO

Security pack

For IT, information security and data protection reviewers

Invigilo Technologies Pte Ltd | Version 1.0 | October 2026

This pack sets out how Invigilo is deployed, where video and data are processed and stored, the certifications Invigilo holds and the controls behind them. It is written to answer the first round of questions in a vendor security review. Detailed evidence, including the Statement of Applicability and ISMS policies, is shared under NDA on request.

1. Certifications

Certification	Detail
ISO/IEC 27001:2022	Certificate of Registration No. 721055, issued by Guardian Independent Certification Pte Ltd, an SAC-accredited certification body and IAF MLA member. Initial certification 7 February 2025, valid to 6 February 2028.
Certified scope	"Provision of Information Technology Consultancy", quoted as it appears on the certificate.
Management system scope	The ISMS Scope Document defines the in-scope organisation as the whole company, with no department, process or location excluded.
Certification audit	Stage 2 audit held 24 to 27 January 2025. Closed with zero major and zero minor nonconformities.
CSA Cyber Trust mark	Cyber Security Agency of Singapore, Practitioner tier, Certificate No. 726284. Issued 13 January 2025, valid to 12 January 2028. Scope: "Provision of Information Technology Consultancy (except Cybersecurity)".

Both certificates carry QR codes and can be checked on the public SAC and IAF CertSearch registers. The address on both certificates is Invigilo's previous office at 71 Ayer Rajah Crescent. The company moved to Block 81 Ayer Rajah Crescent #01-65, Singapore 139967, in July 2026.

Not held

Invigilo does not hold SOC 2 Type I or Type II, ISO/IEC 27017, ISO/IEC 27018, CSA STAR registration, MTCS or PCI DSS. Independent assurance is provided through ISO/IEC 27001:2022 certification and the CSA Cyber Trust mark at Practitioner tier.

2. Deployment options

The deployment model is chosen site by site and decides most answers in a security review, so it is agreed first.

Model	Where AI runs	Where data is stored	Typical use
Hybrid	Server in the site office	Dashboard and reports on Microsoft Azure in the client's region. Video stays on site.	Most sites
On-premise	Server on the client's site or vessel	Client-owned server only. No cloud connection unless the client enables it.	Closed networks, offshore and remote assets
Cloud	Microsoft Azure in the client's region	Microsoft Azure in the same region	Well-connected sites with no on-site hardware

What travels where, in the hybrid model

- **Cameras to server.** Existing IP cameras stream over RTSP or ONVIF on the site's own network to the server in the site office. Continuous video does not leave the site.
- **Server to dashboard.** Only events leave the site: a frame, a short clip, the camera and the time. They are sent over TLS to the dashboard hosted in the client's region.
- **Alerts.** Alerts fire on the local network first, so detection and on-site alerting keep working without an internet connection. Records hold on site until the link returns.
- **Accounts.** No accounts are required on the client's domain or directory. Users sign in to the Invigilo application, and the client's administrators manage their own users through role-based access.

In the on-premise model there is no outbound path for video or detection data, so data residency is met by architecture. In the hybrid and cloud models the hosting region is fixed at implementation and can be written into the service agreement.

3. Data protection

- **Encryption in transit.** Application traffic is served over TLS 1.2 or higher. Remote support sessions use an encrypted zero-trust tunnel with per-device authorisation.
- **Encryption at rest, cloud.** Cloud storage and database services apply platform-managed AES-256 encryption at rest. Credentials are stored salted and hashed.
- **Segregation.** On-premise and hybrid deployments use a dedicated server per client, so no other customer's data is present on that hardware. Cloud deployments run as single-tenant instances.
- **Retention.** Retention periods are set by the client. Expired clips and images are deleted automatically on that schedule.
- **Data loss prevention.** Invigilo does not run a dedicated DLP product. Data leakage prevention is implemented through the Information Classification, IT Security and Access Control policies, assessed as fully implemented in the Statement of Applicability.
- **Exit.** A documented decommissioning procedure covers removal of software and models, erasure of storage in line with NIST SP 800-88, revocation of all Invigilo access, and a signed certificate of data destruction.

4. Privacy

- Invigilo operates under Singapore's Personal Data Protection Act and applies equivalent controls where GDPR obligations arise. A Data Protection Officer is appointed.

- The client remains the data controller for its footage and detection records.
- Face recognition is an optional module, off by default, and switched on only if the client decides.
- Faces, bodies and backgrounds can be blurred per camera before anything is stored.
- Reports are by area, crew and condition. Invigilo does not rank individual workers.
- Use of client footage for model training is set out in the contract and requires the client's written approval.

5. Access control and security operations

- **Access management.** Joiners, movers and leavers are governed by the Access Control Policy. Least privilege applies, privileged accounts are issued separately and approved individually, and access rights are reviewed periodically. Only the engineers assigned to a client hold access to that client's system.
- **Authentication.** Multi-factor authentication is enforced on Invigilo corporate systems. The application password policy is configurable to the client's own standard.
- **Vendor remote access.** Routine operation needs no Invigilo access. For diagnostics, tuning and updates, access is initiated by the client, time-boxed, limited to named engineers and logged. Invigilo uses a zero-trust mesh VPN by default and can use the client's own remote access broker instead. Sites that require no remote path can be supported through scheduled site visits.
- **Logging and monitoring.** A SIEM collects and correlates logs across corporate endpoints, servers and cloud infrastructure, with weekly log review. Monitoring is run by Invigilo's IT function in Singapore and is not a 24-hour staffed SOC.
- **Endpoint protection.** Advanced endpoint protection is deployed on corporate assets and servers, with CIS Benchmark Level 1 hardening applied to endpoints.
- **Application audit log.** The application records sign-ins, failed attempts, configuration and role changes, alert acknowledgement and closure, report generation and data export, with a timestamp and the acting user.
- **Updates.** Application and model updates are delivered as versioned containers with rollback, at times agreed with the client so that monitoring is not interrupted without notice.

6. People, development and continuity

- **Screening.** Candidates are checked for identity, right to work, past employment and references, and declare no criminal record in the application form. All staff are bound by confidentiality obligations.
- **Training.** Security awareness training is mandatory on joining and repeated annually.
- **Development.** Code is peer reviewed before merge, dependencies are tracked for known vulnerabilities, and changes are tested in a separate environment before release. Development follows OWASP secure coding practice. Formalising the secure development lifecycle controls is an active workstream in the ISMS improvement programme.
- **Production data.** Client production data is not copied into development or test environments.
- **Incident management.** A documented procedure covers detection, severity classification, containment, recovery, client notification and post-incident review. The notification period is agreed as a contract term.
- **Continuity.** On-premise and hybrid deployments keep detecting and alerting without any connection to Invigilo, so a disruption at Invigilo does not stop safety monitoring on site. A business continuity plan is maintained within the ISMS.

7. Security reviews and questionnaires

Invigilo completes client security questionnaires, third-party risk assessments and data protection forms as part of onboarding. The following are available on request, under NDA where marked.

Document	Availability
ISO/IEC 27001:2022 certificate and CSA Cyber Trust certificate	On request
Statement of Applicability (93 Annex A controls)	Under NDA
ISMS policies, including access control, encryption, incident management and business continuity	Under NDA
Architecture and data flow for the chosen deployment model	During scoping
Completed client security questionnaire	During onboarding

Send requests to inquiries@invigilo.sg.