Security and compliance overview

Certification, platform access and evidence for your vendor security review.

ISO/IEC 27001:2022 certified ISMS

Spacera Pty Ltd's information security management system is certified to ISO/IEC 27001:2022 by Insight Assurance.

The scope of the certification is the Information Security Management System supporting the provision of the Spacera Apollo platform. Functional Areas that support the ISMS are HR, Finance, IT, Engineering, Sales and Executive Management.

The certification applies to Spacera's ISMS. It does not certify the Apollo product or individual services.

Certificate	IS-IA-2026-10-15-01
Initial issue	15 October 2026
Expiry	14 October 2029
Next surveillance	14 October 2027

SOC 2 Type 2

Examination in progress. Contact our security team for the current status and availability of evidence.

Encryption and access controls

API traffic uses TLS 1.2 or later. Stored operational data and integration credentials are encrypted at rest using AES-256.

Role-based access controls govern customer and partner access. Customer data is logically separated by tenant. Administrative actions and Emily's automated actions are logged.

Understand your deployment

Integration access and write actions

Cloud integrations use vendor-supported APIs with OAuth authorisation, API keys or other vendor credentials, depending on the integration. Revoke authorisation or rotate credentials using the vendor's administration tools.

Photon provides monitoring functionality. Vendor-granted permissions can include write access even where a Spacera feature only reads data. Automated remediation is available on Mission Control and HyperCare. Remote device control is in a limited pilot for selected customers; confirm vendor and action availability with your partner before purchase.

Cloud APIs and optional Satellite

Cloud-to-cloud integrations require no on-premises agent or inbound firewall rules. An optional Apollo Satellite collector can extend monitoring to supported LAN-only devices. Its deployment and outbound connectivity requirements are agreed with your network team.

Data boundaries and location

Apollo processes device health, status, configuration and room metadata. It does not record or read meeting audio, video, chat or transcripts. Account information, onboarding records, support communications and usage data are described in our Privacy Policy.

Apollo uses Microsoft Azure. EU, UAE and US telemetry regions are planned, not generally available. Confirm the available region, residency, retention, deletion and recovery requirements with our team during procurement.

Request evidence

Email security@spacera.io with your name, organisation, work email and the documents you need. Our security team verifies the requester, confirms availability and confidentiality/NDA terms, then shares approved evidence directly.

Evidence	Access
ISO/IEC 27001:2022 certificate	On request following verification
Architecture and integration permissions	On request under NDA
Statement of Applicability and selected policy/control evidence	On request; release terms confirmed individually

Current information: spacera.io/security
Security: security@spacera.io
Privacy: compliance@spacera.io