SECURITY COMMITMENT.

ARES HORIZON

Customer Security & Data Protection Principles

November 2026



antoni@areshorizon.com

areshorizon.com

CUSTOMER SECURITY & DATA PROTECTION PRINCIPLES

Security Commitment

01 / OUR SECURITY COMMITMENT

At Ares Horizon, we recognize that security, confidentiality, and data sovereignty are critical for organizations operating in the defence and aerospace industries. Our platform is designed around security-by-design principles, enabling customers to maintain control over sensitive contractual, supplier, and operational information.

02 / DATA PROTECTION & DEPLOYMENT SECURITY

On-premises or secured cloud

Ares Horizon supports customer-controlled on-premises and appropriately secured cloud deployments. The controls and data-handling principles relevant to each option, including the safeguards shared by both models, are summarized below.

DEPLOYMENT OPTIONS & SAFEGUARDS

ON-PREMISES

- Customer-controlled infrastructure.
- Local AI can keep data, prompts, and outputs within the customer environment.
- No general public internet access required; approved endpoints only where needed.

CLOUD

- Appropriately secured cloud environment under the agreed deployment architecture.
- Inbound access can be limited to approved customer office or VPN IP ranges.
- Outbound connectivity can be limited to approved data sources, AI providers, update services, and operational endpoints.
- External AI providers may be used where their terms prohibit model training on customer content, with data minimization and anonymisation before transfer.

SHARED SAFEGUARDS

- Enterprise SSO and role-based access control.
- No standing access to customer data or environments.
- Security-by-design development and customer-authorized support access.

SECURITY AT A GLANCE

01 CUSTOMER CHOICE

Choose a customer-controlled on-premises environment or an appropriately secured cloud deployment aligned to the agreed architecture.

02 CONTROLLED CONNECTIVITY

On-premises deployments can operate without general public internet access. Cloud access can be limited to approved customer office or VPN IP ranges and approved service endpoints.

03 PRIVATE AI PATHWAYS

Local AI can keep data within the customer environment. Where external models are used, provider terms, data minimization, and anonymisation controls apply.

04 AUTHORIZED ACCESS

Enterprise SSO and role-based access controls support user governance. Ares Horizon has no standing access; support access requires explicit customer authorization.

03 / SECURITY FRAMEWORK ALIGNMENT

Ares Horizon's security practices are being developed with reference to internationally recognized frameworks:

NIST Cybersecurity Framework 2.0	Cybersecurity governance, risk management, protection, detection, response, and recovery.
CIS Critical Security Controls v8.1	Technical security safeguards, system hardening, vulnerability management, and access control.
OWASP ASVS 5.0	Secure application development, authentication, authorization, and application security verification.
NIST AI Risk Management Framework	AI-related risk management, governance, privacy, and trustworthiness.

These frameworks guide our security program and technical practices. References to these frameworks do not represent independent certification or verification of full compliance.

04 / ISO/IEC 27001:2022 CERTIFICATION ROADMAP

Target period | Milestone

Ares Horizon is establishing an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022, with the objective of obtaining independent certification. An external certification audit is currently anticipated between December 2026 and January 2027.

November 2026	ISMS scope, governance, risk assessment, security policies, and Statement of Applicability
November - December 2026	Security control implementation, ISMS operation, and evidence collection
December 2026	Internal audit, management review, and corrective actions
December 2026 - January 2027	Anticipated external certification audits - Stage 1 and Stage 2
Following external audit	Certification decision, subject to successful audits and certification body approval

EXTERNAL AUDIT TIMING

External certification audit timing is anticipated and remains subject to audit readiness, availability, and certification body approval.

05 / TRANSPARENCY & SHARED RESPONSIBILITY

Ares Horizon is committed to transparent security practices and clear allocation of responsibilities between the platform provider and its customers. For on-premises deployments, infrastructure security, network configuration, and operational responsibilities are defined as part of the agreed deployment model. Additional security information and technical documentation may be provided during customer security assessments.

Security is a fundamental design principle, not an optional feature.