

CUSTOMER-FACING SECURITY OVERVIEW

Operational AI needs operational trust.

MAIA is designed for customer-controlled deployment, transparent data flows, auditable actions and configurable human oversight across ship-management workflows.

Customer data remains customer data.

AIA Core Technologies does not use customer operational or personal data for advertising, marketing profiling, lead generation, resale, or disclosure to third parties for their own independent purposes.

1. DATA PRINCIPLES

Broad operational access. Controlled use.

MAIA may need access to broad customer-authorised information sources - including shared mailboxes, manuals, PMS data, document libraries, crew records and operational files - so that it can answer questions and complete real workflows across departments.

That access is governed by the customer's approved scope. Where technically possible, only information relevant to the current task is retrieved and sent onward for model processing.

01**Customer-controlled environment**

MAIA can be deployed on a dedicated customer-controlled VM/server with customer-managed databases and document storage.

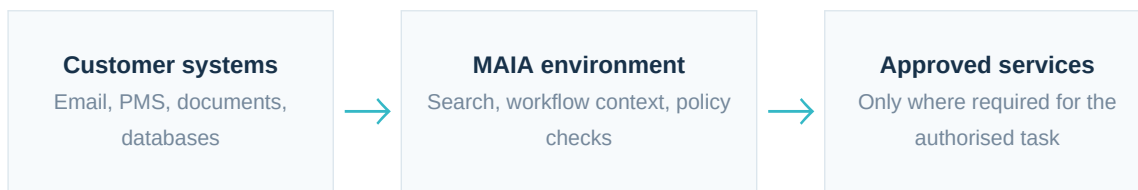
02**Authorised sources**

The customer decides which systems, mailboxes, repositories and workflows MAIA is allowed to access.

03**No marketing use or resale**

Customer data is not used to build advertising audiences, unrelated marketing profiles or commercial datasets for sale.

2. TYPICAL DATA FLOW



Key design principle

Broad search capability is separated from outbound disclosure. MAIA can search across authorised sources without automatically sending entire mailboxes or repositories to an external AI provider.

3. DEPLOYMENT ARCHITECTURE

Keep the operational core under customer control.

MAIA is designed to support private deployment while still allowing carefully controlled use of external services where they are required for the agreed solution.

Private deployment

Core application components, operational databases and document indexes can remain inside a dedicated customer-controlled environment.

Controlled outbound access

Outbound network access can be restricted to approved services needed for the deployment, reducing unnecessary exposure.

Customer-authorised support

Remote AIA support can be enabled only when authorised by the customer and can be time-bounded and auditable where practical.

Credential separation

Passwords, API keys and system credentials are designed to remain outside prompts, documents and normal application logs.

4. TECHNICAL & ORGANISATIONAL CONTROLS

Controls matched to the deployment.

Encryption	TLS for data in transit and encrypted storage where supported by the customer environment.
Roles & permissions	Different users and workflows can receive different read, write, execute and approval authority.
Audit trail	Material actions, approvals, overrides and system interactions can be logged without unnecessarily storing full sensitive content.
Retention & deletion	Retention rules for MAIA-held data, temporary artifacts and logs are agreed for the deployment.
Backups & recovery	Backup, recovery and update procedures align with the customer's infrastructure and operating model.
Incident response	Suspected incidents are contained, investigated and escalated to the agreed customer contact without undue delay where relevant.

5. AI MODEL PROCESSING

External model providers are treated as service dependencies, not data owners.

Some deployments may use an external AI model provider to perform authorised processing. In that case, only the information needed for the task should be sent where technically possible, and the provider is documented as an approved subprocessor where applicable.

Where the OpenAI API is used, API inputs and outputs are not used to train OpenAI models by default unless the customer explicitly opts in. Retention settings depend on the selected endpoint and account configuration.

No advertising use	No resale	Approved subprocessors	Controlled outbound access
--------------------	-----------	------------------------	----------------------------

6. DATA PROTECTION DOCUMENTATION

Document the real deployment before production data is connected.

For a live pilot involving personal or confidential business data, AIA Core Technologies and the customer should document the agreed processing scope and the controls actually enabled in the environment.

DPA	Defines controller/processor roles, processing instructions, confidentiality, subprocessors, deletion and incident cooperation where applicable.
TOMs	Describes the technical and organisational measures actually enabled for the customer's deployment.
Data Flow Diagram	Shows what MAIA reads, where data is stored, which services receive data and why.
Subprocessor List	Identifies approved external providers used to deliver the service.
Retention Schedule	Records agreed retention and deletion rules for logs, temporary artifacts and MAIA-held information.

7. CUSTOMER CONTROL

Security settings follow the customer's operating model.

- Customers approve the systems and data sources MAIA can access.
- Approval gates can be required for sensitive or high-impact actions.
- Write and execute permissions can be narrower than read/search permissions.
- Access can be revoked when a workflow, integration or pilot ends.

8. INCIDENT RESPONSE

Reduce risk, detect issues and react quickly.

- Contain the affected integration or credential.
- Preserve relevant logs and evidence.
- Rotate or revoke compromised secrets.
- Assess the data and systems potentially affected.
- Notify the agreed customer contact without undue delay where relevant.

For customer IT, security or DPO review

A deployment-specific Security Pack can be prepared for a pilot, including the agreed DPA, TOMs, data-flow diagram, subprocessor list and retention rules. Security questions: privacy@aia-core.com.

This overview is intended for customer security evaluation and does not replace deployment-specific contractual documentation.