

KII BUSINESS OS / DATA MANAGEMENT PLAN

Your clients' data stays yours, and stays in Switzerland.

This plan defines how KII data is hosted, mirrored, accessed, logged, retained, and disposed of during the 90-day engagement and after exit. Agency MIOSA works inside KII's own data center. Your systems are mirrored read-only, agents only propose changes, and an authorized KII role approves every write to a production system.

ON-PREM BY DEFAULT

Runs in your data center

Operations run on KII infrastructure. There is no public cloud dependency for operational data.

MIRROR ONLY

Read-only by design

Source systems are mirrored read-only. Current tools keep running, with no disruption to live operations.

HUMAN APPROVAL

No silent writes

Every change to a production system is proposed, reviewed, and approved by an authorized KII role first.

NO TRAINING ON YOUR DATA

Prompts and actions are logged

KII data is never used to train a third-party model. Every interaction is written to the audit trail.

PROVIDER

Agency MIOSA, a registered United States company

CLIENT

KII, Switzerland

DOCUMENT

v1.0 for client review, October 6, 2026

INSIDE THIS PLAN

01 Principles and data classes

02 Residency and hosting

03 Access and governance

04 Mirroring and write approval

05 Models and AI policy

06 Logging, retention, incident response

07 Exit, disposal, and legal basis

Acceptance and signature

FIVE PRINCIPLES, SIX DATA CLASSES

Know what data we hold, and the single rule that governs it.

01 MINIMUM NECESSARY

We access the least data needed to deliver the engagement, and nothing more.

02 ON-PREM BY DEFAULT

KII data stays on KII infrastructure. Copies elsewhere need KII's approval.

03 READ BEFORE WRITE

Mirrors are read-only. Production changes need an authorized KII approval.

04 NAMED ACCESS

Named people hold individual accounts. There are no shared credentials.

05 REVERSIBLE EXIT

At exit we revoke every credential and return or delete every copy.

THE THROUGHLINE

If a handling rule cannot be satisfied, the work stops until it can. We do not trade governance for speed.

DATA CLASS	WHERE IT LIVES	WHO CAN ACCESS	HANDLING RULE
KII business data Contracts, commercial terms, finances	KII systems, inside the KII data center	Named KII roles, plus named Agency MIOSA personnel where the work requires it	Reached through a read-only mirror. No external copy without KII's written approval.
KII client operational data Network signals, tickets, cases, configurations	KII source systems: Autotask, the KII ERP, ticketing, and time billing	Named KII operators and approvers	Read-only mirror. Changes to production only through KII approval.
Personal data KII employees and client contacts	KII systems, inside the KII data center	Named KII roles only	Minimized to what the task needs. Never copied off KII infrastructure except as approved.
Time and billing data	KII time billing and ERP systems	Named KII roles, plus finance where the work requires it	Read-only mirror. No external copy without KII's written approval.
Documentation and source code	KII repositories and the KII documentation store	Named engineers and the KII owners	Held in KII's own repository. KII owns its fork of the platform and all KII-specific work.
Model prompts and outputs, and logs	KII infrastructure	Named KII roles and the Agency MIOSA delivery lead	Logged in the audit trail. Retained per KII policy. Never used to train third-party models.

ON-PREMISES BY DEFAULT

No client data leaves your infrastructure without your written approval.

COMMITMENTS

- The platform runs on-prem in KII's own data center.
- No client data leaves KII infrastructure without KII's written approval.
- Remote work by Agency MIOSA happens only through KII-approved access methods into KII's environment. We do not ask for direct internet exposure of your systems.
- There are no copies of KII data on Agency MIOSA systems, except as KII explicitly approves for a defined purpose and period.
- Subprocessors: none by default for operational data.
- Any later subprocessor requires KII's prior written approval before it can touch KII data.

SWISS AND EU ALIGNMENT

Built to align, not to replace advice

The plan is built to align with the Swiss Federal Act on Data Protection (the revised FADP, in force since September 2023) and the EU GDPR. KII's counsel determines the applicable legal position.

WHERE THE DATA IS

Residency

Operational data remains on KII infrastructure, located in Switzerland. The platform has no public cloud dependency for operations.

WHY ON-PREM

Your clients' data stays in your estate

Your clients' operational data is already inside your perimeter. We keep it there. Nothing about the engagement requires it to move.

Scope of this document: this plan states our operational commitments. It is not legal advice. Where a legal obligation applies, KII's counsel leads and we follow KII's instruction.

No certification claims: this plan does not claim ISO 27001, SOC 2, or any other certification that Agency MIOSA does not hold. If KII requires a specific certification, we will state plainly whether we hold it before any commitment is made.

LEAST PRIVILEGE, NAMED PEOPLE, PERIODIC REVIEW

Governance at three levels: user, role, and data.

LEVEL	WHAT IT CONTROLS	HOW IT IS ENFORCED
User	Who can sign in	Every person has an individual named account. Shared and generic logins are not used.
Role	What a person can see and do	Role permissions map each person to specific modules and allowed actions.
Data	Which records a person can reach	Data scope is applied per record and per workspace, so access follows the person and the task.

01

Named personnel

Only named Agency MIOSA personnel receive access, each through an individual account.

02

Least privilege

Each account holds the minimum access its task requires, and nothing broader.

03

Access reviews

Agency MIOSA and KII review all access at each milestone, and remove what is no longer needed.

REVOCATION

Access ends when the work ends

All Agency MIOSA access is revoked at the end of the engagement. If KII stops after Milestone 1, access is revoked at pilot exit, and KII keeps everything delivered to that point.

CREDENTIALS

Secrets never travel by email

Credentials live in a KII-approved secret store on KII infrastructure. They are never emailed, never shared between people, and removed at exit.

KII retains authority over access: KII can require the removal of any account, at any time, for any reason. We act on that instruction without delay.

READ-ONLY MIRRORS, HUMAN-APPROVED WRITES

Every change to production passes through a person you authorize.



No agent writes directly to production. There is no path around human review. The agent can propose, prepare, and explain, but it cannot apply a change on its own.

No disruption by design. Mirroring means the platform works from a copy while your current tools stay live. If a mirror cannot be built safely, we plan around it with KII before any change.

WHAT THIS DELIVERS IN PHASE 1

The mirror layer for Autotask, the KII ERP, ticketing, and time billing is configured and accepted in Milestone 1. The approval gate and its audit record are configured and accepted in Milestone 2, before Operations goes live with real users.

YOUR MODEL, YOUR HARDWARE, YOUR RULES

Operations run on your internal model. Frontier models stay out of your client data.

RULE	COMMITMENT
Operations model	Operations run on KII's internal model, served via vLLM on KII infrastructure. No operational request needs an external provider.
Frontier models	Frontier models are used only for research, only with non-sensitive data, and only with KII's approval for that specific use.
Training	No KII data is used to train, fine-tune, or improve a third-party model, and no KII data is sent to a provider for that purpose.
Logging	Prompts, outputs, and the actions taken from them are logged in the audit trail, so any result can be traced to its input and its approver.

WHAT WE WILL NOT DO

Five hard limits

- Send client operational data to a frontier provider.
- Train or fine-tune a third-party model on KII data.
- Let an agent apply a production change on its own.
- Reuse KII data to serve another client.
- Hold a copy of KII data outside the approved scope.

RESEARCH USE

Non-sensitive data only

When a research question needs a frontier model, we use non-sensitive or synthetic material, and we get KII's approval first. Client operational data is never the input.

REPLACEABLE BY DESIGN

No lock-in to a provider

The model is a component, not the system. KII can change the model, the hardware, or the provider without losing the platform, the data, or its records.

ACCOUNTABLE BY DEFAULT

Every access and every approval leaves a record you can inspect.

AUDIT TRAIL

Who, what, when, and why

- Every access to KII data, by named account.
- Every agent proposal and its evidence.
- Every approval, edit, or rejection, with the approver's identity.
- Every change applied to a production system.

RETENTION

Per KII policy

Records are retained for the period KII sets in its policy. Nothing is retained beyond that period, and nothing is kept after exit except as the plan and KII's instruction require.

INCIDENT RESPONSE

Notification within 24 hours

Agency MIOSA notifies KII without undue delay, and within 24 hours of becoming aware of an incident affecting KII data.

COOPERATION

We help you respond

Agency MIOSA cooperates with KII's investigation and remediation, and provides the information KII needs to meet its own notification duties.

What counts as an incident: any confirmed or suspected unauthorized access to, disclosure of, loss of, or alteration of KII data, including anything caused by an agent, a credential, or a mirror.

One log, two readers: the audit trail is available to KII at any time, and KII can export it. Access is not self-reported; it is measured from the record.

CLEAN EXIT, IN WRITING

Exit returns everything, removes every credential, and proves it.

EXIT AND DISPOSAL

- On termination, or after pilot exit, Agency MIOSA returns or deletes all KII data and credentials it holds within 14 days.
- Agency MIOSA confirms the return or deletion in writing.
- KII keeps everything delivered to the point of exit, including its fork of the platform and all KII-specific work.

LEGAL BASIS

- A mutual NDA is signed before any data access.
- Agency MIOSA is a registered United States company and provides its registration documents together with the NDA.
- KII remains the controller of its data. Agency MIOSA acts only on KII's instructions, and only for the engagement.

EXIT CHECKLIST

- ☐ All Agency MIOSA access revoked
- ☐ All KII data returned or deleted
- ☐ All credentials removed from the secret store
- ☐ Deletion confirmed in writing to KII
- ☐ Audit trail handed to KII
- ☐ Source and documentation remain in KII's repository

The exit rule: nothing of KII's stays with us unless KII says so in writing. The default is removal.

ACCEPTANCE

FOR AGENCY MIOSA

Roberto H. Luna, Principal Architect and Engagement Lead

Name _____

Title _____

Date _____

FOR KII

Dr. Reza Kordi, Managing Director

Name _____

Title _____

Date _____