

KII CUSTOM MODULE DEVELOPMENT ON BUSINESSOS / DATA MANAGEMENT PLAN

How KII data is handled, in two clearly separated zones.

This plan states exactly where KII data lives, who can reach it, and how it is removed. The KII production platform runs on KII infrastructure and stays there. The engagement is a separate zone: MIOSA's team works from MIOSA-controlled machines and accounts using commercial AI services, so KII data and code made available to MIOSA may be processed outside Switzerland, including in the United States. There is no air gap. Restricted Data is the exception, and it never leaves KII infrastructure.

ZONE 1 / YOUR PLATFORM

Runs on your infrastructure

Operations run on KII hardware and KII's internal model. There is no public cloud dependency for operational data.

READ-ONLY MIRRORS

No silent writes

Current systems are mirrored read-only. Every change to a production system is approved by an authorized KII role first.

RESTRICTED DATA

Never leaves your estate

KII may classify any data as Restricted. Restricted Data is never sent to a third-party AI provider.

NO TRAINING

On any model

KII data is not used to train any model, and MIOSA selects providers whose commercial terms do not permit training on submitted data.

PROVIDER

MIOSA LLC, a Texas limited liability company

CLIENT

KII, Switzerland

DOCUMENT

v1.0 for client review, October 6, 2026

MIOSA LLC. Agency MIOSA is the delivery practice of MIOSA LLC.

INSIDE THIS PLAN

01 Two zones: where the work happens

02 Principles and data classes

03 Restricted Data and the data-flow map

04 How MIOSA uses AI in delivery

05 The KII production platform

06 Access, governance, and audit

07 KII's responsibilities and incidents

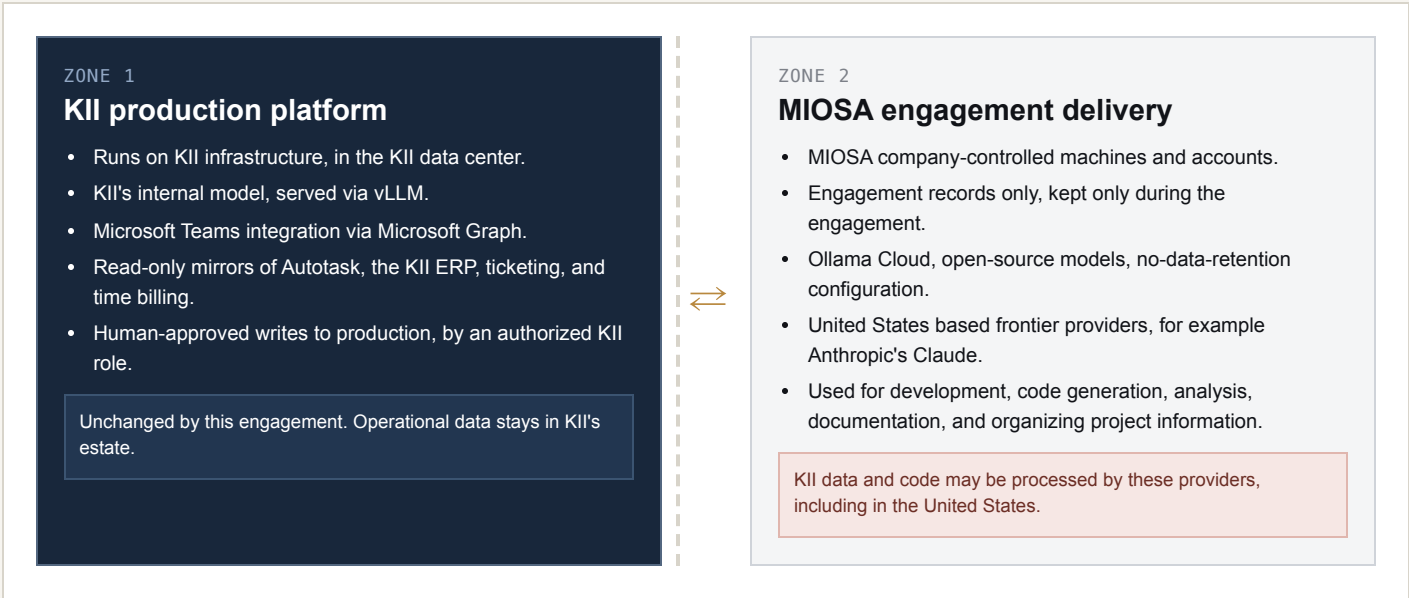
08 Lifecycle, retention, and exit

09 Exit, disposal, and acceptance

TWO ZONES, CLEARLY SEPARATED

The production platform is one zone. The engagement delivery is another.

Read this page first. Almost every question about data handling is answered by which zone the work sits in.



No air-gap guarantee. This is the honest position. MIOSA cannot guarantee an air-gapped engagement. If a body of work must not leave Switzerland, KII classifies it as Restricted Data, and it is handled only on KII infrastructure.

What does not change. The platform KII's team uses every day runs on KII hardware, on KII's internal model, and inside KII's perimeter. Zone 1 is not where MIOSA's AI tools run.

How the two zones meet: KII shares the data and code the engagement needs. Deliverables flow back into KII's own repository. MIOSA's AI tools operate on MIOSA-controlled machines and accounts, never inside the KII production platform.

QUESTION	ZONE 1: KII PRODUCTION PLATFORM	ZONE 2: MIOSA ENGAGEMENT DELIVERY
Who operates it	KII, with MIOSA engineers working under KII's access rules.	MIOSA, on MIOSA company-controlled machines and accounts.
What is stored there	Operational data, mirrors, prompts, outputs, and the audit trail.	Engagement records only, and only during the engagement.
Does data leave it	No. Operational data stays on KII infrastructure.	Yes. Data may be processed outside Switzerland.
Restricted Data	The only permitted home for Restricted Data.	Restricted Data never enters Zone 2.

SIX 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 TWO ZONES

Production data stays on KII infrastructure. Engagement records live on MIOsa-controlled machines for the engagement only.

03 READ BEFORE WRITE

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

04 RESTRICTED MEANS RESTRICTED

Any data KII classifies as Restricted never reaches a third-party AI provider.

05 NAMED ACCESS

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

06 NO TRAINING

KII data is not used to train any model, and providers are chosen whose terms do not permit it.

DATA CLASS	WHERE IT LIVES	WHO CAN ACCESS	HANDLING RULE	MAY MIOsa'S AI TOOLS PROCESS IT?
KII business data Contracts, commercial terms, finances	KII systems, inside the KII data center	Named KII roles	Reached through a read-only mirror. Changes to production only through KII approval.	Yes, unless KII classifies it Restricted
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.	Yes, unless KII classifies it Restricted
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 KII approves.	Yes, unless KII classifies it Restricted
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 BusinessOS and all KII modules.	Yes, unless KII classifies it Restricted
Model prompts, outputs, and logs	KII infrastructure for the production platform	Named KII roles and the MIOsa delivery lead	Logged in the audit trail. Retained per KII policy. Never used to train any model.	Yes, unless KII classifies it Restricted
Restricted Data Any data KII classifies as Restricted	KII infrastructure only	Named KII roles	Never sent to a third-party AI provider. Handled only on KII infrastructure, or only with KII's internal model.	No. Never.

WHERE EVERY CLASS OF DATA ACTUALLY GOES

One class never leaves your infrastructure. Everything else has a named path.

ON KII INFRASTRUCTURE / ZONE 1

01 SOURCE

Source systems

Autotask, the KII ERP, ticketing, and time billing keep running as they do today.

02 MIRROR

Read-only mirrors

A read-only copy of each source system is held inside the KII environment.

03 WORKSPACE

KII workspace

People and agents work in the same project workspace, with role-based visibility.

04 MODEL

KII internal model

Operations requests are served on KII hardware through vLLM. No external provider is needed.

05 APPROVAL

Human-approved writes

An authorized KII role approves every change before it reaches production.

MIOSA ENGAGEMENT DELIVERY / ZONE 2

01 SHARED

Shared for the engagement

KII data and code made available to MIOSA under this plan, for the engagement only.

02 MACHINES

MIOSA machines and accounts

Engagement records are kept only on MIOSA company-controlled machines and accounts.

03 OLLAMA

Ollama Cloud

Open-source models under a no-data-retention configuration, for development and analysis.

04 FRONTIER

United States providers

For example Anthropic's Claude, for development, code generation, analysis, documentation, and organizing project information.

Restricted Data does not enter Zone 2. KII may classify any data as Restricted. Restricted Data is never sent to a third-party AI provider and is handled only on KII infrastructure, or only with KII's internal model. KII decides the classification and tells MIOSA which classes are Restricted; MIOSA follows that instruction for the whole engagement.

WHAT CROSSES

Only the KII data and code KII makes available for the engagement, and only for the duration of the engagement.

WHAT DOES NOT CROSS

Restricted Data, production credentials, and any data KII has not chosen to share.

WHAT COMES BACK

Deliverables and source, into KII's own repository. KII keeps its own copies of everything.

DATA	PATH DURING THE ENGAGEMENT
KII operational data	Stays in Zone 1. Read through the mirrors, served by KII's internal model, and changed only through the approval gate.
KII data shared with MIOSA	Enters Zone 2 on MIOSA-controlled machines, and may be processed by Ollama Cloud or a United States based frontier provider.
Deliverables and source	Written into KII's own repository. Because KII holds its own copies, exit never removes the outcome of the work.

HONEST DISCLOSURE

What MIOSA's team uses, what for, and what it means for KII data.

TOOL OR PROVIDER	WHAT IT IS USED FOR
KII's internal model via vLLM	Serving the KII production platform on KII infrastructure. This is the operations model, and this engagement does not change it.
Ollama Cloud, open-source models	Running open-source models under a no-data-retention configuration, for development and analysis work by the MIOSA team.
United States based frontier providers, for example Anthropic's Claude	Development, code generation, analysis, documentation, and organizing project information. These providers are United States based, so KII data and code made available to MIOSA may be processed in the United States.

THE BENEFIT

Substantially faster delivery

A small team working with AI tools delivers substantially faster, and at lower cost, than a manual team of the same size. That is a large part of why the 90-day timeline and the price are what they are.

THE RISK

Processing happens outside Switzerland

KII data and code made available to MIOSA may be processed by third-party providers, including in the United States. MIOSA cannot guarantee an air-gapped engagement. For any body of work that must not leave Switzerland, KII classifies it as Restricted Data.

No training on KII data. MIOSA does not use KII data to train any model, and selects providers whose commercial terms do not permit training on submitted data.

No certification claims. This plan does not claim ISO 27001, SOC 2, or any other certification MIOSA does not hold. If KII requires a specific certification, MIOSA will state plainly whether it holds it.

Not legal advice, and a clear liability line. This plan states operational commitments, not legal advice. Where a legal obligation applies, KII's counsel leads and MIOSA follows KII's instruction. MIOSA chooses third-party AI providers with reasonable care and configures them as described, but is not responsible for a provider's own breach beyond that. The overall liability cap in the Services Agreement applies.

WHAT COULD GO WRONG	WHAT CONTROLS IT
KII data processed outside Switzerland	KII classifies anything that must not leave as Restricted Data. Restricted Data is never sent to a third-party AI provider.
A provider changes its commercial terms	MIOSA selects providers whose terms do not permit training on submitted data, and reviews those terms when they change.
A provider suffers a breach	MIOSA notifies KII without undue delay, cooperates with the response, and the overall liability cap in the Services Agreement applies.

READ-ONLY MIRRORS, HUMAN-APPROVED WRITES

Every change to production passes through a person you authorize.

01 SOURCE Source system Autotask, the KII ERP, ticketing, and time billing keep running as they do today.	02 MIRROR Read-only mirror A read-only copy of the source system is held inside the KII environment.	03 PROPOSAL Agent proposal An agent prepares a proposed change, with the evidence and reasoning behind it.	04 REVIEW Human review An authorized KII role reviews the proposal, then approves, edits, or rejects it.	05 APPLY Apply to production Only an approved change is applied to production, by the KII operator.	06 AUDIT Audit record Every proposal, approval, and applied change is written to the audit trail.
---	--	--	--	---	---

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. 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.

Source layer	Autotask, the KII ERP, ticketing, and time billing keep running exactly as they do today. Nothing is replaced during the 90 days.
Mirror layer	Read-only copies are held inside the KII environment. This layer is configured and accepted in Milestone 1.
Approval layer	The approval gate and its audit record are configured and accepted in Milestone 2, before Operations goes live with real users.
Workspace layer	People and agents work in the same project workspace. Sessions are visible to the team according to role, and another person can take over a task with full context.

WHAT KII CONTROLS The approval role, the scope of each mirror, and every credential. KII can withdraw any of them at any time.	WHAT AN AGENT CAN DO Read the mirrors, prepare a proposal, explain its reasoning, and draft the work. It cannot apply a change.	WHAT THE RECORD SHOWS Every proposal, approval, and applied change, so any result traces back to its input and its approver.
--	---	--

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

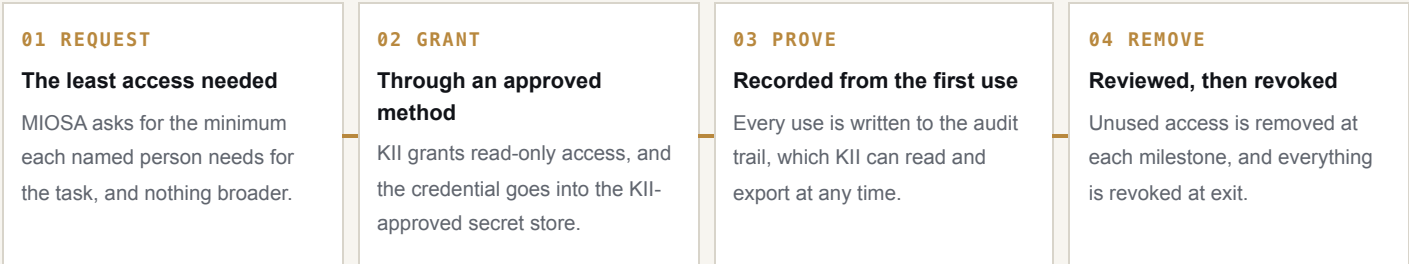
REVOCATION
Access ends when the work ends
All MIOSA access is revoked at the end of the engagement. If KII stops after Milestone 1, access is revoked at pilot exit, and KII keeps everything delivered to that point.

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.

The audit trail, in one place. Every access to KII data by named account, every agent proposal and its evidence, every approval, edit, or rejection with the approver's identity, and every change applied to production is written to the audit trail. KII can read and export it at any time. Access is not self-reported; it is measured from the record.

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

THE ACCESS LIFECYCLE



WHO DECIDES WHAT

KII classifies its data and notifies its clients. MIOSA follows both.

KII'S RESPONSIBILITIES

- Classify its data, including anything it designates as Restricted Data, and tell MIOSA which classes are Restricted.
- Provide any notices or consents its own clients require, including cross-border disclosure under the Swiss FADP and the EU GDPR.
- Set retention periods and deletion instructions under its own policy.
- Name the security and data owner who approves access methods and handling rules.

MIOSA'S RESPONSIBILITIES

- Process KII data only as this plan and KII's instructions allow, and only for the engagement.
- Keep engagement records on MIOSA company-controlled machines and accounts, only during the engagement.
- Never send Restricted Data to a third-party AI provider, and never train any model on KII data.
- Notify KII of an incident without undue delay, and cooperate with KII's response.

INCIDENT NOTICE PATH

01 DETECT

Confirmed or suspected

Any confirmed or suspected unauthorized access to, disclosure of, loss of, or alteration of KII data.

02 NOTIFY

KII security owner

MIOSA notifies KII without undue delay, and within 24 hours for an incident in MIOSA's own systems.

03 ASSESS

Joint assessment

MIOSA provides the information KII needs to judge impact and meet its own notification duties.

04 DECIDE

KII decides

KII decides what its own clients are told, and when. MIOSA supports that decision.

Remediation: MIOSA cooperates with KII's investigation and remediation, and removes or rotates the credentials or access involved.

Scope of an incident: anything caused by an agent, a credential, a mirror, or a third-party provider acting on KII data shared for the engagement.

RECORD	WHAT IT CONTAINS	WHERE IT IS KEPT	RETENTION
Audit trail	Every access, proposal, approval, and applied change, with identities attached.	KII infrastructure	Per KII policy
Decision log	Each ruling KII makes on access, data, and scope, with the owner named.	KII workspace	Per KII policy
Engagement records	Recordings, transcripts, documents, exports, and working copies.	MIOSA-controlled machines	Engagement only
Deletion certificate	Written confirmation that KII data and working copies have been deleted.	Provided to KII on request	KII keeps it

FROM KICKOFF TO A DELETION CERTIFICATE

Engagement records live for the engagement, then leave on a schedule.

01 KICKOFF

Classification and access

Data classes are agreed with KII, Restricted Data is identified, and access is granted through KII-approved methods only.

02 ENGAGEMENT

Processing during delivery

MIOsa processes data as this plan describes. Records, recordings, transcripts, documents, exports, and working copies stay on MIOsa-controlled machines and accounts.

03 END

Termination or completion

Access is revoked and MIOsa stops processing new KII data. KII keeps everything delivered to that point.

04 DELETE

Within 30 days

MIOsa deletes all KII data and working copies, including copies of deliverables it holds. KII keeps its own copies.

05 CERTIFY

Written certificate

MIOsa confirms the deletion in writing on KII's request.

BACKUPS

Only with your written permission

MIOsa keeps backups only with KII's written permission, and only for the period KII approves. Without that permission, the 30-day deletion covers backups as well. There is no default retention.

RETENTION DURING THE ENGAGEMENT

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 the engagement except as KII approves in writing.

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

Pilot exit: after Milestone 1 acceptance, KII may stop with no further fees, keep everything delivered to that point, and MIOsa disposes of KII data as this plan states.

DELETED BY MIOsa

All KII data, all working copies, and the copies of deliverables MIOsa holds. The default outcome is removal.

KEPT BY KII

The BusinessOS fork, all KII modules, configuration, documentation, and KII's own copies of deliverables.

KEPT ONLY WITH PERMISSION

Backups, only with KII's written permission, and only for the period KII approves. There is no default retention.

CLEAN EXIT, IN WRITING

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

EXIT AND DISPOSAL

- On termination, or after pilot exit, MIOSA revokes every credential it holds and deletes all KII data and working copies, including copies of deliverables it holds, within 30 days.
- MIOSA certifies the deletion in writing on KII's request.
- KII keeps everything delivered to the point of exit, including its fork of BusinessOS and all KII modules, and keeps its own copies of deliverables.

ACKNOWLEDGMENT

This Data Management Plan is incorporated into the Agreement as Exhibit B and is accepted when the Agreement is signed. It is not signed separately. This plan is not legal advice; KII's counsel determines the applicable legal position.

EXIT CHECKLIST

- ☐ All MIOSA access revoked
- ☐ All KII data and working copies deleted
- ☐ All credentials removed from the secret store
- ☐ Deletion certified in writing on request
- ☐ Audit trail handed to KII
- ☐ Source and documentation remain in KII's repository

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

HANDOVER PACKAGE

Source, configuration, and the BusinessOS fork, delivered into KII's own repository.

ACCESS REMOVAL

Every MIOSA account and credential revoked, and the removal confirmed in writing.

RECORDS

The audit trail and the decision log, handed to KII so nothing about the engagement is lost.

ACCEPTANCE

This plan is incorporated into the Agreement as Exhibit B and is accepted when the Agreement is signed. There is no separate signature page for this plan. KII signs the agreement once, with the Statement of Work as Exhibit A and this plan as Exhibit B.