Handover Checklist

This document records what the client receives at the end of an Onebit-AI engagement, who owns each item after handover, and what remains open. It is complete when every table row has an owner and every check item is ticked or marked "not applicable".

At a glance

Everything you receive at the end of an engagement and how ownership is transferred.

- You own code, prompts, evals, data and infrastructure accounts
- Tables for repositories, environments, credentials and documents
- Ends with a dated sign-off and a 30-day support period by default

Read in 8 minutes. The tables are filled in during the last week of a build.

How to use this document

We start filling this in during the final two weeks of the engagement, not on the last day. Each section is a list of things that must be true before we sign off. Tick items only after you have verified them yourself: log in, open the repo, run the restore. Where an item does not apply to this engagement, write "N/A" and a short reason. Unresolved items go into the open-items table in section 08 with a named owner and a date.

Engagement	
Client	
Onebit-AI lead	
Client technical owner	
Target handover date	

01 Ownership statement

The client owns everything we produced for this engagement: source code, infrastructure definitions, prompts, agent configurations, evaluation sets and eval results, data pipelines, designs, and documentation. We retain no licence to the client's deliverables beyond what is needed to provide agreed support.

Repositories are created in the client's own organisation from day one. If an engagement started in an Onebit-AI account for practical reasons, the repositories are transferred (not forked or copied) so that history, issues and settings move with them.

Third-party components we selected are listed below with their licences. The client is responsible for ongoing compliance with those licences; we confirm at handover that nothing we introduced carries a licence incompatible with the client's

stated use.

COMPONENT	VERSION	LICENCE	USED FOR	NOTES
Illustrative example: PostgreSQL	16.x	PostgreSQL Licence	Primary datastore	Managed by cloud provider

- [ ] Contract clause on IP ownership matches the statement above

Reference the clause number in the agreement

- [ ] No Onebit-AI personal or shared accounts remain as owners of any client asset
- [ ] Model provider and SaaS subscriptions are in the client's name and billed to the client

02 Repositories and access

Every repository, package registry, container registry and design file is listed. "Owner after handover" is a named person or team in the client's organisation, never "Onebit-AI".

ITEM	LOCATION	OWNER AFTER HANDOVER	STATUS
Illustrative example: API service repo	github.com/example-co/api	Platform team	Transferred, admin verified

- [ ] Client holds admin on every repository and registry

Verified by the client, not by us

- [ ] Branch protection and required reviews are configured and documented
- [ ] CI/CD pipelines run under client-owned service accounts

- [ ] Onebit-AI accounts are downgraded to read-only or removed on the agreed date

Default: removed at the end of the support period, adjust per engagement

- [ ] Design source files (if any) are in the client's design tool workspace

03 Environments and infrastructure

Each environment is listed with its cloud account, region and the person who pays for it. Infrastructure is defined as code; anything created by hand is listed as an exception with a plan to bring it under code or a reason not to.

ENVIRONMENT	CLOUD ACCOUNT / PROJECT	REGION	BILLING OWNER	IAC LOCATION
Development				
Staging				
Production				

- [ ] Cloud accounts are owned by the client's organisation with client-controlled root/owner credentials

Root credentials are held by the client only; we never hold them

- [ ] Domains are registered under the client, with auto-renew on and a client contact on the registrar account
- [ ] DNS zones are in a client-owned account and every record is documented
- [ ] TLS certificates renew automatically; the renewal mechanism is named in the runbook
- [ ] A fresh environment can be created from IaC alone; we demonstrated this once during handover
- [ ] Manually created resources are listed as exceptions
- [ ] Budget alerts are set on each cloud account and route to the client

Manual exceptions (resource, why, plan) _____

04 Credentials and secrets

Secrets are never sent by email, chat or shared documents. They move through the client's secret manager or a one-time, expiring share link that we confirm was opened. After handover the client rotates every secret we ever had access to, so that nothing we once knew still works.

SECRET / CREDENTIAL	STORED IN	HOLDER AFTER HANDOVER	ROTATED AFTER HANDOVER
Illustrative example: Model provider API key (prod)	Cloud secret manager	Platform team	Yes, date:

- [ ] Inventory above covers API keys, database passwords, signing keys, webhook secrets, OAuth client secrets and service-account keys
- [ ] No secret is committed to any repository; history was scanned and the scan result is attached
- [ ] Every secret we had access to has been rotated by the client

Default: within 5 business days of handover, adjust per engagement

- [ ] Applications read secrets from the secret manager, not from files or environment variables set by hand
- [ ] Access to the secret manager is limited to named client staff and service accounts
- [ ] MFA is enabled on every account listed in sections 02 and 03

05 Documentation set

Documentation lives beside the code it describes, in the repository. The runbook is written so that an engineer who has never seen the system can deploy, roll back and recover it.

DOCUMENT	LOCATION	PRESENT	REVIEWED BY CLIENT
README (setup, run locally, test, deploy)			
Architecture overview (diagram + one page of prose)			
Runbook (deploy, rollback, common failures, recovery)			
Architecture decision records (ADRs)			
API specification (OpenAPI or equivalent)			
Data model and migration history			

DOCUMENT	LOCATION	PRESENT	REVIEWED BY CLIENT
Prompt and agent catalogue (each prompt, its purpose, model, version, owner)			
Evaluation reports (eval sets, latest results, how to re-run)			
Third-party licence list (from section 01)			

For AI components: the catalogue must let the client change a prompt, re-run the evals and see whether quality moved. If that loop cannot be run by the client alone, the handover is not complete.

06 Operations

From the handover date the client's team receives alerts, owns the on-call rota and can restore the system without us.

- [ ] Monitoring dashboards exist for availability, latency, error rate and, for AI components, cost per request and eval score trend
- [ ] Alerts route to a client-owned channel or paging tool; no alert goes only to an Onebit-AI address
- [ ] Alert thresholds and what to do for each alert are in the runbook
- [ ] Backups run on a schedule and a restore test was performed with the client present

Record the date, the backup used and the time to restore

- [ ] Cost dashboard shows cloud and model-provider spend by environment; the client can open it
- [ ] Log retention and access are set to the client's policy
- [ ] On-call expectations are agreed: who responds, in what hours, and how escalation works

Restore test date and result _____

Alert destination _____

On-call owner after handover _____

07 Knowledge transfer

Knowledge transfer is a recorded walkthrough, at least one live session with the people who will run the system, and a defined window for questions. The support period has a start and end date agreed in writing.

ACTIVITY	DATE	ATTENDEES	RECORDING / NOTES LOCATION
Recorded walkthrough (architecture, deploy, runbook)			

ACTIVITY	DATE	ATTENDEES	RECORDING / NOTES LOCATION
Live session 1			
Live session 2 (if needed)			
Client-led deploy observed by us			

Q&A window (start / end) _____

Support period (start / end) _____

Support channel and response target _____

Default: a 30-day support period from final acceptance, with questions answered by email within 2 business days. Onebit-AI and the client agree the actual terms per engagement.

08 Sign-off

Sign-off means the client has verified sections 01 to 07 and accepts the open items below with their owners and dates. Open items do not block sign-off unless marked "blocking".

OPEN ITEM	OWNER	DUE DATE	BLOCKING?

Handover date _____

Onebit-AI access removal date _____

Support period end date _____

Secret rotation confirmed by (name, date) _____

Signed for Onebit-AI · name · date

Signed for the client · name · date