

AI Operations Assistant Security Standard

NigelBuilds builds and manages AI Operations Assistants for service businesses. This is the NigelBuilds deployment standard: the rules every client install is built to. No client environment is running yet, so each control is marked STANDARD or ROADMAP. It is not a compliance certification.

Architecture

01	Your team	People approve, edit or reject from email, Slack, Teams or phone.
02	Dedicated server	Standard: a separate virtual machine for each client. Nothing shared with another client.
03	Docker container	The assistant runs inside a locked container with only the tools you approved.
04	Assistant	Runs your jobs and follows the permission rules for your plan.
05	Scoped credentials	Per-client keys and OAuth apps you own, with the narrowest access that works.
06	Your business systems	Email, calendar, CRM, accounting and documents, each connected on purpose.

Controls (deployment standard)

Separate environment per client STANDARD Each client install gets its own server and container. Client data is never placed next to another business's data.	Your credentials, your accounts STANDARD Integrations are set up through OAuth apps and API keys created in your own accounts where the provider allows it, so you can revoke any of them without calling me.
Approvals before changes STANDARD Changes to a system go through the permission level on your plan. Money, deletions and security settings are blocked on every plan.	Audit trail STANDARD Reads, drafts, approvals and actions are logged with a timestamp and who approved them.
Spend caps STANDARD Model and tool usage runs under a hard monthly cap you set, and pauses instead of running past it.	Kill switch STANDARD One switch stops the assistant. You can pull it, and so can I.

Monitoring

STANDARD

Heartbeat, scheduled job success, expiring tokens, tool failures and spend alerts are checked daily.

No unrestricted execution

STANDARD

The assistant never runs with open-ended permission in a production system. Every tool is allowlisted and scoped.

No consumer AI accounts

STANDARD

Production clients run on business API accounts only, never a personal ChatGPT or Claude subscription.

Nightly backups with restore tests

ROADMAP

Nightly backups of memory, jobs and logs, with scheduled restore tests. The automated backup and restore-test tooling for client environments is not built yet.

Offboarding export and revocation

ROADMAP

An export of memory, jobs and logs, credential revocation and environment destruction. Done by hand today. Automated tooling is not built yet.

Runtime portability

ROADMAP

The design avoids lock-in to one model or runtime vendor. Swapping the runtime for a client has not been tested yet.

Permissions by plan

Action	Basic	Pro	Max
Read email, calendar and documents	READ	READ	READ
Reply to a customer email	DRAFT	APPROVAL	EXECUTE
Create or update a CRM record or task	DRAFT	APPROVAL	EXECUTE
Book or move a calendar event	DRAFT	APPROVAL	APPROVAL
Send an invoice reminder	DRAFT	APPROVAL	EXECUTE
Run a browser workflow in a web portal	NEVER	APPROVAL	APPROVAL
Issue a refund or move money	NEVER	NEVER	NEVER
Delete records or email	NEVER	NEVER	NEVER
Give medical, legal or financial advice	NEVER	NEVER	NEVER
Change passwords, users or security settings	NEVER	NEVER	NEVER

Implemented and tested today (public demo only)

- Synthetic data only, with no code path to client or production data
- Per-session, per-visitor and global daily rate limits, tested by pushing past them
- An on/off switch that returns recorded responses when the demo is disabled
- No send, charge or delete tools exist in the demo

Plain limits

- No client environment is running yet. The controls above are the NigelBuilds deployment standard, not a record of past operation.
- NigelBuilds does not hold a SOC 2, ISO 27001 or HITRUST certification. I will not claim one.
- HIPAA work is limited. Clinical records are out of scope unless a signed BAA and a written scope cover it. Operations work that does not touch protected health information is the default.
- Model providers process the text the assistant sends them under their business API terms. I pick providers that do not train on API data by default and tell you which ones are in use.