Security and procurement pack

Everything a risk, compliance or IT reviewer needs to assess NorthCape, in one document, with no form in front of it. Where we do not hold something, this pack says so rather than writing around it.

How to read this. Sections 1 to 3 describe where your data goes under each deployment option. Sections 4 to 7 cover subprocessors, access, incidents and the data processing agreement. Section 8 is fifteen questions worth putting to any AI implementation vendor, with our own answers beside them.

1. Deployment options

Three options. The boundary is a decision made with you during solution design, before an agent touches real work, and it is written into the engagement.

A
NORTHCAPE OPERATED

B
YOUR CLOUD TENANCY

C
YOUR OWN HARDWARE

LAYER	A: NORTHCAPE OPERATED	B: YOUR CLOUD TENANCY	C: YOUR OWN HARDWARE
Application runtime	Fly.io, Sydney region	Your cloud account, in the region you choose	Your servers
Database and files	NorthCape managed, Sydney	Your account, your encryption keys	Your storage
Model inference	AWS Bedrock ap-southeast-2, or a private model we host	Bedrock in your own account, or a private model in your account	Private model on your hardware
Credentials to your systems	Held by NorthCape in a secret store, scoped per connection	Held in your own secret store	Never leave your network
Administrative access	NorthCape named individuals	NorthCape named individuals, granted and revoked by you	You. NorthCape only when you grant it, for as long as you grant it
Network egress	To the named subprocessors in section 4 only	Whatever your own network policy allows	Can be none. Air-gapped operation is supported
Typical fit	Fastest to stand up. Suits teams with no cloud platform function	Suits an existing cloud estate with its own controls	Suits a data classification that cannot leave the premises

2. Data boundary matrix

What leaves your environment and what never does, for each option. If anything elsewhere on our site appears to say otherwise, this table is the controlling statement.

DATA	A: NORTHCAPE OPERATED	B: YOUR CLOUD TENANCY	C: YOUR OWN HARDWARE
Document and matter content	Leaves, to the NorthCape environment in Sydney	Never leaves your cloud account	Never leaves your network
Prompt content for a commercial model	Leaves, to AWS Bedrock in ap-southeast-2	Leaves, to Bedrock in your own account and region	Never leaves. Private models only
Model outputs	Returned to the NorthCape environment	Stay in your account	Stay on your hardware
Credentials to your systems	Held by NorthCape, encrypted at rest, scoped per connection	Never leave your secret store	Never leave your network
Audit trail of agent actions	Stored with NorthCape, exportable to you at any time	Stored in your account	Stored on your hardware
Operational telemetry: latency, token counts, error codes	To NorthCape. Contains no document content	To NorthCape only if you enable it. Off by default	Off unless you choose to export it
Email notifications to your staff	Leaves, to Resend in the United States	Resend, or your own SMTP relay	Your own SMTP relay
Personal data of your staff, for approvals	Name and work email in the NorthCape environment	Stays in your account	Stays on your hardware

"Never leaves" means there is no configured network path out. It is a statement about the architecture, not an undertaking about our conduct. Where the table says data leaves, it names where it goes, and you can refuse that specific choice during solution design.

3. Model and retention

Models

MODEL TYPE	WHERE INFERENCE RUNS	PROVIDER RETENTION OF PROMPTS AND OUTPUTS	TRAINING USE
Claude via AWS Bedrock	ap-southeast-2, Sydney	None. Bedrock does not store prompts or completions	No
Private or self-hosted open weight model	Wherever you deploy it, including your own hardware	Not applicable. There is no third party provider in the path	No

MODEL TYPE	WHERE INFERENCE RUNS	PROVIDER RETENTION OF PROMPTS AND OUTPUTS	TRAINING USE
No model: deterministic rules	In the application runtime	Not applicable	Not applicable

The model used for each task is named in the week 2 solution design, so a commercial model can be accepted or rejected task by task rather than discovered later. Where a task can run on a private model, it can be configured to run only on a private model.

Retention

DATA CLASS	RETENTION	WHERE	CONFIGURABLE
Prompt and output content	Not retained beyond the task	Held only for the duration of the request	Yes, where a workflow requires an output be saved as a record
Application logs, containing no document content	90 days, then deleted	The deployment environment	Yes, shorter or longer by agreement
Audit trail of agent actions and approvals	Life of the engagement, then exported to you or deleted	The deployment environment	Yes
Database backups	7 days of point in time recovery	The deployment region	Yes
Website enquiries and booking records	Kept until you ask us to delete them	NorthCape environment, Sydney	Deleted on request, without conditions

4. Subprocessors

The complete list. If a subprocessor is not named here, it is not in the path of your data.

SUBPROCESSOR	PURPOSE	REGION	WHAT REACHES THEM	APPLIES TO
Amazon Web Services, Bedrock	Model inference for tasks using a commercial model	ap-southeast-2, Sydney	Prompt content and model output for that task	Options A and B, and only where a commercial model is chosen
Fly.io	Application and database hosting	syd, Sydney	Application data at rest and in transit	Option A only
Resend	Transactional and notification email	United States	Recipient name, email address and the content of the message sent	Any option where email notification is enabled. Replaceable with your own SMTP relay
Microsoft, Bookings and Microsoft 365	Scheduling meetings booked from our	Australian Microsoft 365	Name, email and anything typed into	The northcape.tech website only. Not part of any client

SUBPROCESSOR	PURPOSE	REGION	WHAT REACHES THEM	APPLIES TO
	website	tenancy	the booking form	deployment

- New subprocessors are notified in writing 30 days before they are used, and you may object.
- Resend is the only subprocessor outside Australia. Where offshore email processing is unacceptable, your own relay replaces it and the list becomes wholly Australian.
- We do not use offshore contractors or an offshore development team. Delivery is done by the named engagement team.

5. Access and approval model

CONTROL	HOW IT WORKS
Who has access	Named individuals only, listed in the engagement. In practice that is the two founders plus anyone you have explicitly approved.
How access is granted	Per connection and per system, at the least privilege the workflow needs. Scope is explicit rather than inherited, so it cannot quietly widen.
Authentication	Multi-factor authentication on every account with access to a client environment. No shared logins.
Credential handling	Held in a secret store, encrypted at rest, never committed to a repository, never sent by email and never pasted into a ticket.
Time limits and removal	Access can be time-limited at your request, and is removed within one business day of a request or immediately on termination.
Agent autonomy	Every agent action is either autonomous or approval-gated, set task by task in the solution design. High-stakes actions can stay gated permanently.
Approvals	Each approval records who approved, what they approved and when. An approval gate cannot be bypassed by the agent.
Audit trail	Every action logged: what ran alone, what waited, who approved it and why it escalated. Exportable at any time and yours to keep.
Change record	Changes to an agent's permissions or autonomy are recorded and attributable to a person.

6. Incident response

An incident is any unauthorised access to, loss of, or disclosure of client data, any compromise of a credential used to reach a client system, and any agent action outside its configured boundary that affected client data.

> **We notify you within 72 hours of becoming aware of an incident affecting your data.** The clock starts at awareness, not at occurrence. We will send an incomplete notification inside 72 hours rather than a complete one late, and follow it with updates.

What the notification contains

- What happened, and when we became aware of it.
- The categories of data involved and, as far as known, the volume.
- The likely consequences.
- What we have done to contain it, and what we are still doing.
- A named contact who can answer follow-up questions directly.

How we respond

- **Contain.** Revoke the affected credentials and suspend the affected agent. This happens before analysis, not after it.
- **Assess.** Establish scope from the audit trail and the application logs.
- **Notify.** You, inside 72 hours, at the contact named in the engagement.
- **Remediate.** Fix the cause, restore service, and confirm the fix with you in writing.
- **Review.** A written post-incident review within 10 business days, sent to you whether or not you ask for it.

Under the Notifiable Data Breaches scheme you generally hold the obligation to notify the OAIC and the affected individuals, as the entity with the relationship to them. We support that obligation with the facts and the timeline, and we will not delay your assessment while we finish ours. Report anything you suspect to info@northcape.tech.

7. Data processing agreement summary

The clause headings, and what each one commits us to. We will sign your own data processing agreement. If you do not have one, ours is available on request and this is its shape.

CLAUSE	COMMITMENT
1. Roles, scope and duration of processing	You are the controller and NorthCape is the processor. The categories of data, the purposes and the duration are listed per engagement rather than left general.
2. Instructions and purpose limitation	We process only on your documented instructions and for no other purpose. Explicitly, we do not use your data to train any model or to improve a product.
3. Confidentiality and personnel	Everyone with access is bound by confidentiality that survives the engagement, and access is limited to those who need it to deliver it.
4. Technical and organisational measures	Encryption in transit and at rest, least privilege access, multi-factor authentication, logging, and the retention periods in section 3.
5. Subprocessors	The list in section 4, 30 days written notice of any addition, your right to object, and the same obligations flowed down to each of them.
6. Data subject requests and assistance	We assist with access, correction and erasure requests, and with your privacy impact assessments, within the timeframes the request imposes on you.
7. Personal data breach notification	Notification to you within 72 hours of awareness, with the content listed in section 6, and cooperation with any regulator notification you must make.

CLAUSE	COMMITMENT
8. Return, deletion and audit	Return or deletion of your data at your election within 30 days of termination, written confirmation once done, and your right to request evidence of compliance.

8. Fifteen questions to ask any AI vendor

These are worth putting to every vendor on your shortlist, not only to us. Our own answers sit beside them. Four of the fifteen are a plain no and a fifth is qualified, which is the reason for publishing the list.

#	QUESTION	NORTHCAPE'S ANSWER
1	Where does our data physically go, and can you name every region?	Yes. Section 2 names every destination for each deployment option. Under options B and C the content never leaves your environment. Under option A it sits in Sydney, with inference in ap-southeast-2.
2	Which third parties see our content, and can we veto one?	The four named in section 4, and only those. You can veto any of them during solution design. Vetoing AWS Bedrock means a private model. Vetoing Resend means your own mail relay.
3	Is our data used to train any model, by you or by your providers?	No. Not by us, and Bedrock does not retain prompts or completions or use them for training. This is written into the data processing agreement rather than left to a website page.
4	How long is anything retained, and by whom?	Prompts and outputs are not retained beyond the task. Application logs are 90 days. Backups are 7 days. The audit trail lasts the engagement and is then handed to you or deleted. Full table in section 3.
5	Do you hold ISO/IEC 27001 certification?	**No. We do not currently hold ISO/IEC 27001 certification** and we are not in a certification process. If certification is a hard requirement for your procurement, we will not meet it, and it is better that you know that now than in week six.
6	Do you hold a SOC 2 Type II report?	**No. We have not completed a SOC 2 audit** of any type. What we can offer instead is this document, direct answers to your own questionnaire, and evidence of the controls in section 5.
7	Are you IRAP assessed, or on a government panel?	**No to both.** We are not IRAP assessed and we are not on a Commonwealth or Victorian government panel. Work at a classification requiring either is outside what we can honestly take on today.
8	Has your platform had an independent penetration test?	**No independent penetration test has been commissioned to date.** We will accept and support a test you commission, at your cost, before or during an engagement, and we will remediate what it finds.
9	Do you have written security policies and an information security management system?	Partly, and the distinction matters. We have documented practices for access, credentials, logging, retention and incident response, and they are the ones described here. We do not operate a certified ISMS with an audit programme.
10	Who at your company can access our systems, and how	Named individuals only, currently the two founders plus anyone you approve. Least privilege per connection, multi-factor authentication, and revocable by you within one

#	QUESTION	NORTHCAPE'S ANSWER
	is that controlled?	business day. Section 5 has the detail.
11	Do you have an incident response plan, and what is your notification window?	Yes, summarised in section 6, and the window is 72 hours from becoming aware. That is a contractual commitment in the data processing agreement, not a target.
12	Will you sign our data processing agreement?	Yes. If you do not have one, ours is available and section 7 is its shape. We will not ask you to accept terms you have not read.
13	How are we told when you add a subprocessor?	In writing, 30 days before use, with a right to object. If you object and no alternative exists, you may terminate without penalty.
14	What happens to our data, and to the agent, when we leave?	Your data is returned or deleted at your election within 30 days, with written confirmation. You keep a perpetual licence to the agent configuration, prompts and rules built for you. Under options B and C the agent already runs on infrastructure you control.
15	What is your key person risk, and what insurance do you carry?	**We are a two person firm and that is a real concentration risk.** Both founders can run any engagement, configuration is version controlled and handed over, and options B and C leave the running system in your control. We carry professional indemnity and public liability cover, with certificates of currency on request, and we do not hold a standalone cyber liability policy.

If a vendor answers all fifteen with a yes, ask for the evidence on questions 5 to 8. Certifications are documents with numbers on them. A vendor that holds them can produce them in a day.

Document control

VERSION	1.0
OWNER	NorthCape Technology. Questions to info@northcape.tech.
REVIEW	On any change to the architecture or the subprocessor list, and at least every six months.
STATUS OF THESE STATEMENTS	Descriptions of how the platform is built and operated. Where a statement is a commitment rather than an observation, the notification window and the retention periods in particular, it is carried into the data processing agreement so that it binds.