

# Morning Desk Security Summary

Client records and AI drafting stay in Google Cloud's Sydney region, only the adviser's firm can see them, and nothing reaches a client without the adviser's sign-off. Checked every day, not just promised.

Updated 1 November 2026

For compliance teams



## Built on Google Cloud

Client records and AI drafting in Sydney, with no fallback offshore.



## Encrypted

In transit and at rest, on every page and record.



## Adviser signs off

The desk drafts. Nothing reaches a client until the adviser sends it.

### WHERE CLIENT DATA GOES



## Adviser and team

Google, Microsoft or one-time email link. No passwords stored.



## Morning Desk on Google Cloud, Sydney

Books, notes, call notes, drafts, audit trail

Australia

Encrypted

Backed up daily



## Only the firm

Members see only the desks they are given.



**Live voice, read-aloud and deep research** can run outside Australia. Voice and research get a label such as **Client 1** and holdings, never names or notes. **Strict Australian residency**, one switch in the Trust centre, turns all three off, enforced on the server.

### BUILT ON GOOGLE CLOUD

## Client records sit in Google Cloud's Sydney region, on infrastructure the Australian Government has assessed.

Google Cloud's Australian regions meet the Australian Government's IRAP assessment and its Hosting Certification Framework. The same infrastructure is independently audited worldwide.

### IRAP

Assessed for the Australian Government

### ISO/IEC 27001

Information security management

### SOC 2

Independent controls reports

### Google secures

- Data centres, hardware and the network
- Encryption of everything stored
- The certified infrastructure above

### Vertical AI secures

- Sign-in through the firm's Google or Microsoft account
- Each firm's desk walled off from every other firm
- Client records and AI drafting kept in Sydney
- An audit trail of every draft, sign-off and staff access

The certifications are Google Cloud's and cover its infrastructure, not Morning Desk itself. Compliance teams can request Google's IRAP and SOC reports through Google's Compliance Reports Manager.

### CHECKED EVERY DAY, NOT JUST PROMISED

- **Trust centre** in the desk: a live map of where data is, from the running system's own settings. Plain rules, no AI.
- **Daily check at 7:05am** emails Vertical AI if anything fails or changes.

- **New-device sign-ins** trigger an alert.
- **Staff access** to a desk is written to that desk's own audit trail.
- **Compliance pack:** the map, the checks and the staff-access log, as one PDF.

### THE DETAIL



## Who can see it

- ✓ The firm's signed-in people only, each to their own desks.
- ✓ No passwords stored; the firm's two-step sign-in applies.
- ✓ Firm desks are closed to Vertical AI staff. On early pilot desks, support access is possible and every open is logged.



## How it's protected

- ✓ HTTPS only, encrypted at rest; keys in Secret Manager.
- ✓ Signed sessions that expire; rate limits and cross-site protection.
- ✓ Daily backups, kept 14 weeks.



## What the AI does

- ✓ Drafts and summarises, with sources.
- ✓ The same safety rule on every AI call; checks figures.
- ✗ Never sends to a client. No buy, sell or hold advice.



## The firm's control

- ✓ Initials until compliance approves real names.
- ✓ Export or delete all data any time; deleted on request when a firm leaves.
- ✓ Never used to train AI, by Google or by us.

### WHO WE USE

#### Google Cloud

Hosting, database, AI, voice

Client data, in Australia

#### Firebase Auth

Adviser sign-in (Google)

Adviser email only

#### Stripe

Billing

No client data

#### Resend

Sign-in and alert emails

Adviser email only

### QUICK ANSWERS

#### Used to train AI?

No. Not by Google, not by us.

#### Where is it stored?

Google Cloud in Sydney. Only voice, read-aloud and deep research can run elsewhere, and strict residency switches them off.

#### What if the firm leaves?

Export everything, then we delete it on request.