

How we keep your product secure

Where your data lives and how it comes back to you is in our data handling statement. Your services agreement carries the binding terms.

Hosting	We do not host. Your product runs on accounts in your name, in Australian regions
Multi factor sign in	On every account we use, ours and the ones you give us access to
Passwords	Kept in an encrypted password manager, one folder per client. Never sent by email or chat
Access	Each person has their own login with only the access the work needs. No shared logins
Removing access	When someone leaves your project, and for us all at handover, on your instruction, confirmed in writing
People	Everyone on your project is named in the statement of work and signs confidentiality and IP assignment before they start
Devices	Encrypted, kept up to date, locked when idle
Code	Kept in your own repository. Every change goes through a pull request, automated checks and a separate review pass before it is merged
Sign in, data and payments	Checked against a written list before every release
Secrets	Held in your providers' secret settings, never written into the code
Dependencies	Kept current. Known vulnerabilities are checked before every release
Test data	We build and test with made up data. Our tools, AI included, never see your real records
Backups	Run by your provider. We restore one before each go live to prove it works
Incidents	We tell you within 48 hours of becoming aware and help with the response and any notice the law requires
Handover	The code, account list, credentials, runbook and changelog, so you can run the product without us

Questions to support@lumanworth.com.