



CHAINAGE

BY TEKSWIPE TRAFFIC

 **SECURITY & PRIVACY**

Security & Data Handling

How Chainage protects your projects, your people and your privacy — in plain language, for anyone assessing Chainage for their business.

OUR COMMITMENT

Your information stays yours – and stays safe

Chainage holds information that matters to the businesses that use it: where crews are working, project plans, site photos and documents. We treat it the way we'd want our own treated — kept in Australia, protected at every layer, visible only to the people you choose, and never sold.

This document explains how Chainage stores and secures your data, who can see it, what we can and can't see ourselves, and the controls you have. It's written for anyone assessing Chainage — IT and security teams, procurement, and the people who'll use it every day — and it describes how Chainage works today.

**Hosted in Australia**

Servers, database, photos, files and backups are all in Sydney.

**Encrypted**

Every connection uses HTTPS. Backups are encrypted with AES-256.

**Your data is yours**

You own your content and can export all of it, any time.

**Never sold**

We don't sell or share your data, or use it to train AI.

**Private by design**

Our admin tools don't show the contents of your projects.

**Two-factor sign-in**

App or email codes. Companies can make it compulsory.

**Backed up daily**

Encrypted, kept in Sydney and tested automatically every day.

**Nothing hidden**

Every admin action is logged, and companies see it in their own activity log.

IN THIS DOCUMENT

Questions businesses ask us	3
Where your data lives	4
Who can see what	5
Protecting your account	6
Protecting the platform	7
Backups and recovery	8
Usage analytics: exactly what we see	9
Your data, your control — and what happens if something goes wrong	10



Security and privacy aren't add-ons for us. Every feature in Chainage is built so that your work is visible only to your team and the people you share it with — and so that you can see exactly what happens to your data.

QUICK ANSWERS

Questions businesses ask us

01 How is our data stored and secured?

In a database and private file storage in DigitalOcean's Sydney data centre, reachable only through the Chainage app — which checks your access on every request. Connections are encrypted (HTTPS, TLS 1.2 or newer), passwords are stored only as bcrypt hashes, and daily backups are encrypted with AES-256. Pages 6 to 8 explain the details.

02 Where is it hosted?

In Sydney, Australia: DigitalOcean hosts the server, database, photos, files and backups, and Amazon Web Services sends our emails from its Sydney region. Card payments are handled by Stripe.

03 Who owns the data?

You do. Our Terms of Service state that you own your content, and projects created in a company belong to that company. We use it only to provide the service, and you can export all of it whenever you like.

04 Is it shared, sold or accessed by third parties?

No. We never sell or rent your data, and nothing we can see is shared outside Chainage. Only our hosting provider stores your project data, on our behalf. We'd only disclose information where the law requires it.

05 Which third-party services does Chainage use?

A small number of trusted providers help run Chainage. Page 4 lists each one, what it does, what it receives and where.

06 What policies and documents are available?

This document, our Privacy Policy (chainage.com.au/privacy) and our Terms of Service (chainage.com.au/terms). We're happy to complete security questionnaires — email support@tekswipe.com.au.

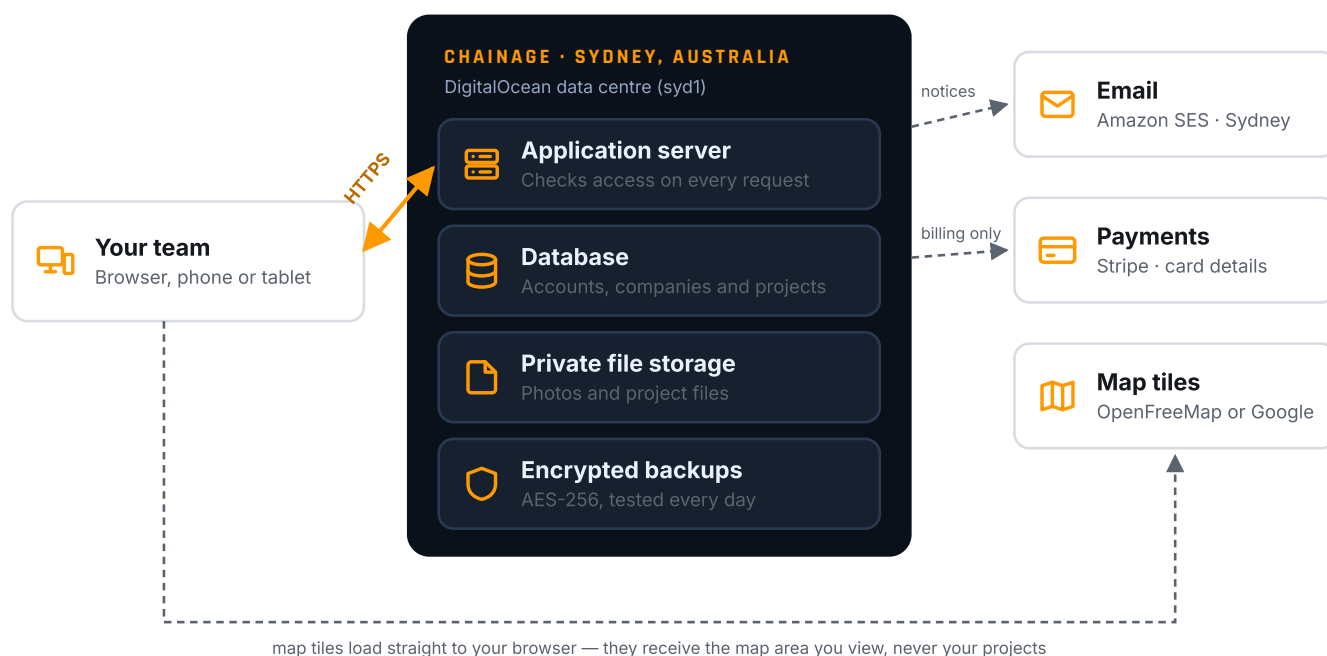
07 Is our data used to train AI, or to give insights to other customers?

No. Your data isn't used to train AI models, and it's never used to give other customers — or anyone else — insight into your work. When you're signed in, the places you look up aren't even recorded in our usage statistics (page 9).

HOSTING & PROVIDERS

Where your data lives

Everything you store in Chainage — accounts, companies, projects, points, ranges, notes, photos, files and backups — is kept in Australia, in DigitalOcean's Sydney data centre. Your devices talk to Chainage over encrypted connections, and only Chainage's own server can reach the database and file storage.



PROVIDER	WHAT IT DOES	WHAT IT RECEIVES	WHERE
DigitalOcean	Hosting, database, private file storage and backups	Your account and project data — stored on our behalf	Sydney, Australia
Amazon Web Services (SES)	Sends Chainage emails	Your email address and the message	Sydney, Australia
Stripe	Card payments and subscriptions	Billing name, email and card details — we never see full card numbers	United States and other regions
Google	Page statistics (Analytics); Maps and Street View if you choose them	Page names only — never map locations, searches or projects. The map area you view, when you use Google maps	United States and other regions
OpenFreeMap	Map tiles	The map area being viewed, requested by your browser	Outside Australia
OpenStreetMap (Overpass) and NHVR	Speed limits and heavy-vehicle routes	The location you selected, when you tap "More information"	Overseas (OSM); Australia (NHVR)

Apart from DigitalOcean storing it for us, none of these providers receives the contents of your projects.

ACCESS

Who can see what

Your team sees what their roles allow and what you share with them. We see what we need to run the service and bill for it — and nothing from inside your projects.

	YOU & YOUR TEAM	CHAINAGE ADMINISTRATORS	OTHER CHAINAGE CUSTOMERS	OUTSIDE COMPANIES
Project contents Points, ranges, notes, photos and files	✓ By role and sharing	✗ Not shown in our tools	✗ Only what you share	✗
Project names and details Name, client, reference, dates	✓ By role and sharing	👁️ Only to restore data you ask for	✗ Only what you share	✗
Account details Name, email and plan	✓ Your company's admins	✓ For support and billing	✗	👁️ Payment and email providers
Usage figures Number of projects, storage used	✓ Your company	✓ For billing	✗	✗
Anonymous usage overview Where the app is used (page 9)	✗ Not shown	👁️ Signed-out visitors only	✗	✗



What our admin tools show

Chainage is run by TekSwipe Traffic. A single administrator account can open the admin console, and only with two-factor sign-in. It shows account details, how many projects an account or company has and how much storage it uses — which we need for billing and support. It doesn't show maps, points, notes, photos or files.



Every action is on the record

Anything an administrator does to someone else's account or company — such as resetting a password, unlocking an account or restoring data — is written to an audit log that can't be edited, and also appears in that company's own activity log as "Chainage support".

An honest note: as with any hosted service, the people who operate the servers could technically reach the database directly. Server access is limited to a single administrator using key-based sign-in only, and it's used to keep the service running — not to look at customer content.

ACCOUNTS

Protecting your account

Most breaches start with a stolen or guessed password. Chainage adds layers so a password alone is never enough — and so you hear about anything unusual straight away.



Password

Checked against a bcrypt hash; wrong guesses count towards the lockout



Second step

Code from an authenticator app or email — or a single-use recovery code



Signed in

New device? You get an email. Tick "remember this device" to skip codes for 30 days



Two-factor sign-in

An authenticator app or 6-digit email codes, plus 10 single-use recovery codes. Required for every administrator.



Company-wide two-factor

Company owners can require it for every member. Anyone without it can't open company data until they set it up.



Lockout protection

Repeated wrong passwords slow down, then lock the account until it's unlocked from an emailed link (see below).



Security alerts by email

Sign-ins from a new device, repeated wrong passwords, a locked account, and any change to the password or two-factor.



Signed-in devices

See every device signed in to your account. Sign one out, or sign out everywhere at once.



Strong passwords

At least 10 characters; common and easily guessed passwords are refused. Stored only as bcrypt hashes.



Roles and permissions

7 built-in roles plus custom roles from 33 permissions. Nobody can grant a permission they don't hold.



Company-managed accounts

With the member's agreement, company admins can unlock the account or reset its password or two-factor. The member is emailed every time.



Share links you control

Limited to chosen phases and layers, with optional password and expiry, and revocable any time. Companies can require both.



Activity log

Project and company actions are recorded with who did what and when, for your admins to review.

WRONG PASSWORDS IN A ROW

1-4

Normal sign-in

5

Wait 30 s · email sent

6

Wait 1 min

7

Wait 2 min

8

Wait 5 min

9

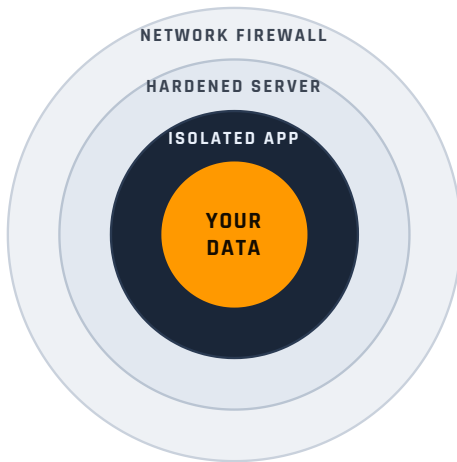
Wait 10 min

10

Locked · unlock link emailed

INFRASTRUCTURE

Protecting the platform



Defence in depth: an attacker would have to get through every layer — the network, the server, the application and then the data itself.

Each layer is protected separately, so a weakness in one doesn't expose the next. The application never runs with administrator rights, and the data it holds is checked against your permissions on every single request.

**Encryption in transit**

HTTPS everywhere (TLS 1.2 or newer), with HSTS so browsers never connect insecurely.

**Encrypted backups**

AES-256-GCM. The key is kept on the server and is never stored with the backups.

**Private files**

Photos and files sit in private storage. Every download checks access first, through a link that expires within 10 minutes.

**Locked-down server**

Firewall open only to the website and key-only administrator access. Password logins are off, and repeated attempts are blocked automatically.

**Automatic security updates**

Installed daily, with an overnight restart when an update needs one.

**Isolated application**

Runs as a restricted account inside a strict system sandbox. Its data files are private to the app.

**Web protections**

Strict content security policy, cross-site request protection on every change, rate limits, and certificates only for our own domains.

**Secrets kept secret**

Keys live in restricted files, never in code. Share-link codes and other secrets are kept out of server logs.

**Checked dependencies**

Every release is scanned for known vulnerabilities and built with a current, supported Go release.

**Monitoring and alerts**

We're alerted automatically if the service goes down, errors appear or resources run high.

RESILIENCE

Backups & recovery

Mistakes and failures happen. Chainage is backed up every day, every backup is encrypted, and every backup is tested — so if something goes wrong we can bring your work back.

**Every night**

2 am Queensland time, a consistent copy of the database is taken.

**Encrypted**

Compressed, then encrypted with AES-256. Unreadable without our key.

**Stored in Sydney**

Kept in private storage, separate from the live database.

**Tested**

Downloaded, decrypted, opened and checked. Stored files are spot-checked.

**Alerted**

We're emailed if a backup or its test ever fails — or doesn't run.

**What we can restore**

A single project — as it was, or as a copy alongside the current version — a single user's account and projects, or the whole system. Deleted photos and files can be brought back for 30 days. Every restore is recorded in the audit log.

**How long backups are kept**

Daily backups are kept for 90 days, so we can go back to any recent day. Deleted data may remain in our backups for up to 12 months before it's gone for good, as our Privacy Policy explains.

AFTER SOMETHING IS DELETED**Day 0**

Deleted in Chainage — gone from the app straight away

30 days

Deleted photos and files can still be restored

Up to 12 months

Deleted data, including photos and files, may remain in our systems and encrypted backups

After that

Gone for good



Backups are encrypted before they leave the server, stored separately from the live database in Sydney, and can't be read without the encryption key.

TRANSPARENCY

Usage analytics: exactly what we see

To decide where to take Chainage next, we look at an overview of *where* the app is used. For example, it showed us where to add council roads first — Chainage now includes Sunshine Coast and Moreton Bay council chainages (zoom in on the Sunshine Coast to see them). Here's exactly what that overview contains.



What we see

From visitors who aren't signed in: where a pin was dropped or a location shared (the first of the day), shared map links that were opened, what was searched for, the type of device and time spent in the app.



What we don't

No names, emails or accounts — visits are grouped by a random code kept in the browser. No IP addresses — each is replaced by a one-way scrambled code before anything is saved. No project data, ever.



Signed in? You're opted out

When you use Chainage signed in to an account — including every paid plan — the places you look up and the searches you make aren't recorded at all. Only anonymous counts remain.

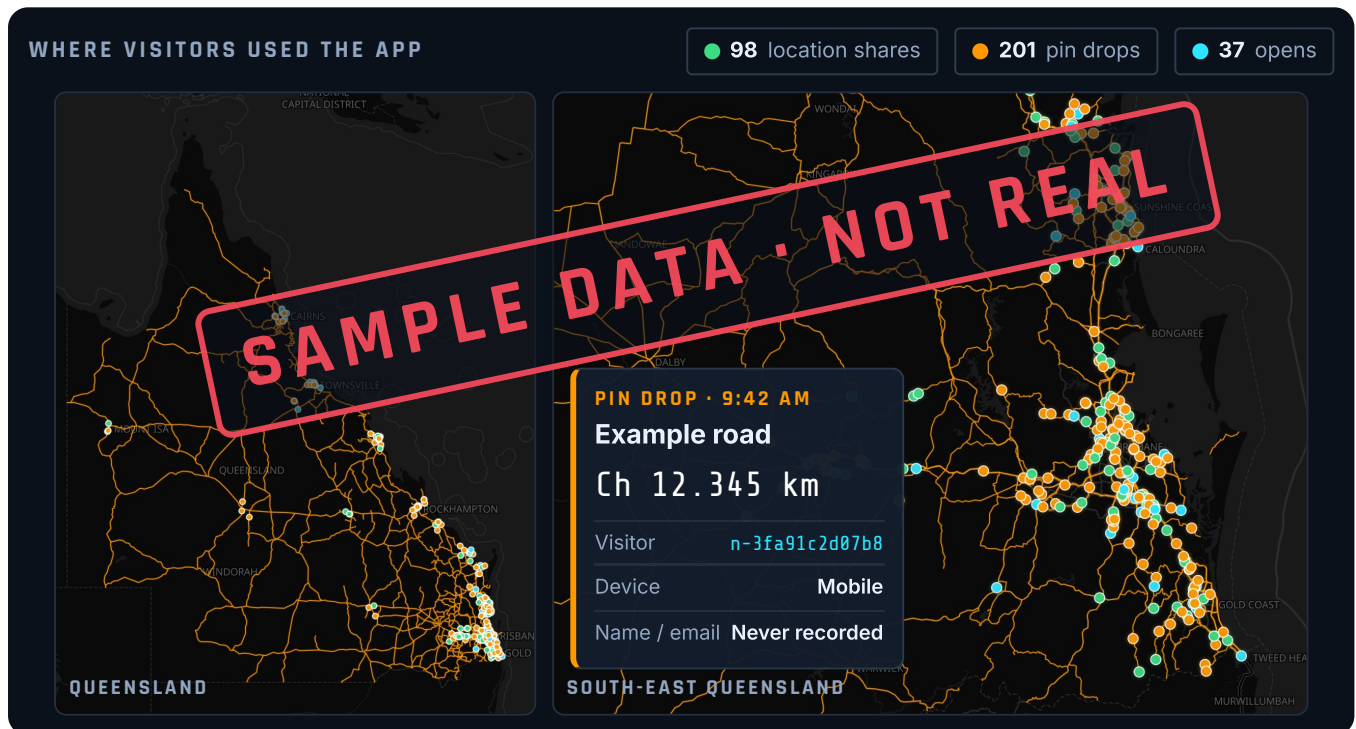


Illustration only. This is a mock-up of our analytics map with made-up sample dots, not real visitor data. The map and the Main Roads network are real; the dots are scrambled. The real map works like this: one dot per pin drop, location share or opened map link from visitors who aren't signed in.

The overview is for our own planning only. It isn't sold or shared with anyone outside Chainage, and it's never used to profile a person or a business. Google Analytics, which we use for page statistics, only ever receives page names — never map locations, searches or link codes.

CONTROL

Your data, your control



Export any time

One click downloads everything — project details, every point and range as GeoJSON (for GIS) and CSV, plus photos and files. For a whole company, or just your own projects.



Delete when you choose

Delete projects at any time. A company owner can delete the whole company, with a 7-day period to change their mind. Ask us and we'll delete your account.



Clear retention

Inactive free accounts are deleted after 2 years, and accounts that have paid after 3 years — always after reminder emails. Active subscriptions are never deleted for inactivity.

If something goes wrong



Detect

Automatic monitoring alerts us to outages, errors and unusual activity.



Contain

We shut off the affected access and change any keys involved.



Investigate

We work out what happened, what was affected and who.



Notify

We tell affected customers and, where required, the OAIC under the Notifiable Data Breaches scheme.



Improve

We fix the cause and update our safeguards.

QUESTIONS OR CONCERNS?

Talk to us

For security questions, questionnaires, data requests or to report a concern, email support@tekswipe.com.au.

Privacy Policy — chainage.com.au/privacy

Terms of Service — chainage.com.au/terms

This document — chainage.com.au/security.pdf



This document describes Chainage as at October 2026. We update it when our practices change — the latest version is always at chainage.com.au/security.pdf. Chainage is a service of TekSwipe Traffic, Queensland, Australia.