

Privacy Policy

Purpose

To define how Kordia collects, stores, shares, manages and protects personal information. Personal information is any information that can identify a person, either on its own or when combined with other information.

Kordia must protect personal information and manage it in accordance with the Privacy Act 2020 (New Zealand) and Privacy Act 1988 (Australia).

Scope

This policy applies to anyone who interacts with Kordia, including employees, contractors, customers, suppliers, consultants, and job applicants.

Statements

Collection

- Kordia will only collect personal information that is necessary for a legitimate business purpose or to meet a legal obligation.
- Where possible, Kordia should collect personal information directly from the individual concerned.

Transparency

- Kordia must be transparent about why personal information is collected, how it will be used, who it may be shared with, and how individuals can access or correct their information.

Fair collection

- Kordia should collect personal information lawfully, fairly, and in a way that respects individual privacy rights.

Protection

- Kordia must protect personal information from loss, unauthorised access, misuse, alteration, or disclosure.

Access

- Kordia must provide individuals with access to their personal information where required by law.

Correction

- Kordia must provide individuals with the opportunity to correct their personal information.

Accuracy

- Kordia must take reasonable steps to ensure personal information is accurate, complete, relevant and up to date before using it.

Keeping information

- Kordia must only keep personal information for as long as it is needed to support business needs or legal obligations.

Using personal information

- Kordia must only use personal information for the purpose it was collected, unless there is a lawful reason to use it for another purpose.

Sharing personal information

- Kordia must only share personal information where there is a legitimate business need, appropriate consent, or a legal basis to do so.

Sharing overseas

- Kordia must ensure appropriate privacy safeguards are in place before personal information is disclosed outside New Zealand.

Unique identifiers

- Kordia must only assign a unique identifier to an individual where necessary to support business operations and protect against mistaken identity.

Exemptions

Kordia does not share personal information unless there is a valid reason to do so.

In some situations, the law may require or allow Kordia to provide information to government agencies, regulators, law enforcement, emergency services, or other authorised organisations. This may include requests made under:

NZ

- Telecommunications (Interception Capability and Security) Act 2013
- Search and Surveillance Act 2012
- Official Information Act 1982

Aus

- Telecommunications Act 1997 (Cth)
- Telecommunications (Interception and Access) Act 1979 (Cth)
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)
- Other Australian laws that require or authorise disclosure to law enforcement, national security agencies, courts, or regulators.

Where this occurs, only information that Kordia is legally required or authorised to disclose will be provided.

Compliance & Monitoring

All employees, contractors, and other workers must comply with this policy.

Approved on: 20/08/2026	Approved by: ELT	Next approval on: 20/08/2027
Version: 3.0	Policy Sponsor: GM Risk & Assurance	Policy Author: General Counsel

Kordia will monitor compliance with this policy and investigate any suspected or actual privacy breaches.

Privacy breaches must be reported promptly through Kordia's incident reporting process.

This policy will be reviewed annually, or earlier if there is a significant change in legal, regulatory, or business requirements.

The General Counsel is assigned the role of Privacy Officer and is responsible for overseeing compliance with this policy.

Responsibilities

Employees

- Must understand and comply with this policy.
- Must protect personal information they access or use as part of their work.
- Must promptly report any suspected or actual privacy breach.

Managers

- Must support compliance with this policy within their teams.
- Must ensure privacy risks and incidents are reported and addressed.

Privacy Officer

- Must oversee compliance with privacy obligations.
- Must provide advice on privacy matters.
- Must coordinate the management of privacy incidents and complaints.



Neil Livingston
Kordia Group CEO

Approved on: 20/08/2026	Approved by: ELT	Next approval on: 20/08/2027
Version: 3.0	Policy Sponsor: GM Risk & Assurance	Policy Author: General Counsel