

Kalgoorlie IT

Privacy & Confidentiality Policy

Version 2.0 - October 2026

This policy explains how KPCD Pty Ltd trading as Kalgoorlie IT (Kalgoorlie IT, we, us or our) handles personal information and protects confidential information encountered while delivering IT, telecommunications, cloud, hosting, cyber security and related services.

1. Purpose

Kalgoorlie IT handles information belonging to customers, their staff, suppliers and other parties as part of normal service delivery. Our objective is to collect and use only the information reasonably required to provide services, operate our business, meet legal obligations and protect our customers and systems.

2. Scope

This policy applies to Kalgoorlie IT personnel, contractors and systems used to collect, access, store, process, transmit or disclose personal or confidential information.

It applies to information handled directly by Kalgoorlie IT and information accessed while supporting customer environments.

3. Information we collect

Depending on the services provided, we may collect or have access to information such as:

- business and personal contact details, account and billing information;
- user, device, licensing, service and support information;
- technical logs, security alerts, configuration information and audit records;
- information supplied in support requests, emails, files or other communications;
- credentials, authentication information or delegated administrative access where reasonably required to deliver a service; and
- personal information contained in customer systems that our personnel may incidentally encounter while providing support.

4. How we use information

We use information only for legitimate purposes connected with our business and the services we provide.

- providing, supporting, maintaining and improving services;
- managing accounts, billing, licensing, suppliers and service contracts;
- monitoring security, investigating incidents and protecting systems;
- communicating with customers and responding to requests;
- meeting legal, regulatory, insurance and contractual obligations; and
- internal administration, quality assurance and service planning.

5. Confidentiality commitment

Customer information is treated as confidential. Our personnel must not access, use, copy or disclose customer information unless it is reasonably required for their role, for service delivery, for an authorised business purpose, or where disclosure is required or permitted by law.

We do not treat access to a customer's systems as permission to inspect unrelated information.

6. Access control

Access is granted on a role-based and need-to-know basis. We use administrative controls designed to limit access to people who require it for their work.

Where practicable, we use named accounts, delegated administrative access, multi-factor authentication and auditable access rather than shared or uncontrolled credentials.

7. Security measures

Kalgoorlie IT uses layered technical and operational safeguards appropriate to the information and systems we handle.

- multi-factor authentication for supported administrative and cloud services;
- endpoint security and managed security tooling where applicable;
- secure remote-access methods and controlled administrative privileges;
- patching, monitoring, logging and vulnerability-management processes;
- backups for systems and workloads specifically covered by an applicable service; and
- reasonable physical, technical and procedural controls for business systems and records.

8. Third-party services and disclosures

We use third-party vendors, cloud providers, carriers, distributors, software providers and professional advisers where reasonably required to deliver services or operate our business.

Information may be disclosed to those parties only to the extent reasonably necessary for that purpose, subject to applicable contractual, confidentiality, privacy and legal obligations.

Some service providers may process or store information outside Australia. Where the Australian Privacy Principles apply, we will take reasonable steps required by law in relation to cross-border disclosure.

9. Data retention and disposal

We retain information for as long as reasonably required for service delivery, business records, contractual requirements, dispute handling, security, backup, legal obligations and other legitimate purposes.

When information is no longer reasonably required and no legal or operational reason requires its retention, we will take reasonable steps to delete, destroy or de-identify it.

10. Security incidents and data breaches

Suspected privacy, confidentiality or data-security incidents are assessed and managed through our incident-response processes.

Where the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth) applies, we will assess suspected eligible data breaches and make notifications where required by law.

Customers are expected to promptly notify us of suspected compromise affecting services we manage or information relevant to our service delivery.

11. Privacy Act and Australian Privacy Principles

Where Kalgoorlie IT is subject to the Privacy Act 1988 (Cth) in relation to particular personal information, we handle that information in accordance with the applicable Australian Privacy Principles.

Nothing in this policy is intended to reduce any privacy right or obligation that cannot lawfully be excluded.

12. Access, correction and privacy enquiries

Individuals may contact Kalgoorlie IT to request access to or correction of personal information we hold about them, subject to any lawful exceptions.

Privacy questions or complaints can be directed to Kalgoorlie IT using the contact details published at kalgoorlieit.com.au. We will review privacy complaints and respond within a reasonable period.

13. Customer information and managed services

For managed customers, Kalgoorlie IT may have privileged or administrative access to systems. That access is provided for service delivery and does not transfer ownership of customer data to Kalgoorlie IT.

Customers remain responsible for deciding what information is stored in their systems, ensuring they have authority to collect and use that information, and informing us of any special handling requirements that are relevant to the services we provide.

14. Policy review

This policy is reviewed periodically and may be updated when our services, legal obligations, security practices or technology change. Material changes will be published or otherwise communicated where appropriate.