DATA USE POLICY

Smithtek Pty Ltd

Effective date	23 September 2026
Data contact	info@smithtek.com.au

Smithtek Pty Ltd (Smithtek, we, us or our) provides hardware, software, communications and cloud-based services for remote monitoring, telemetry, automation and control.

This Data Use Policy explains how data generated, transmitted, stored or processed through Smithtek products and services is handled. It applies to Smithtek products and services including our PLCs, gateways, telemetry equipment, connected devices, cloud platforms, dashboards, software, APIs and associated support services.

This policy should be read together with the Smithtek Privacy Policy, which explains how we collect, use and protect personal information.

1. What we mean by Operational Data

When you use Smithtek products or services, equipment and systems may generate or transmit information about your site, assets, equipment and operations. We refer to this information collectively as Operational Data.

Device and sensor data - such as tank levels, pressures, flow rates, temperatures, equipment status, meter readings, environmental measurements and other information collected from sensors, PLCs, controllers or connected equipment.

Location and site data - such as the location of equipment, monitoring sites, gateways or other assets where location information is provided or enabled.

Control and command data - including commands sent to equipment, setpoints, control actions, schedules and records of remote operation.

Alarm and event data - including alarm conditions, thresholds, equipment faults, notifications, acknowledgement records and event histories.

Device and configuration data - such as device identifiers, communication settings, firmware information, configuration settings and relationships between devices.

Network and diagnostic data - including communication status, signal information, connection logs, device health, errors and diagnostic information used to operate and troubleshoot the service.

Third-party data - information received from equipment, platforms, sensors or services supplied by third parties where those systems have been connected or integrated with Smithtek products or services.

Operational Data may sometimes be associated with personal information, such as a user's name, email address, account or activity. Where information constitutes personal information, it is also handled in accordance with our Privacy Policy and applicable privacy laws.

2. How Operational Data is collected

Operational Data may be collected:

- automatically from Smithtek products, gateways, PLCs, sensors and connected equipment;

- when equipment communicates with a Smithtek cloud platform or other connected service;
- when users enter information, configure equipment or operate devices through a dashboard or application;
- through integrations with third-party equipment, software or services;
- during installation, commissioning, maintenance or technical support; and
- when diagnostic information is generated by our systems.

The type and amount of data collected will depend on the products, services and functionality being used.

3. How we use Operational Data

Smithtek may use Operational Data to:

- provide remote monitoring, telemetry, automation and control services;
- display information through dashboards and other user interfaces;
- transmit commands to connected equipment;
- generate alarms, notifications and reports;
- store historical measurements and operational records;
- operate and maintain connected devices and communications;
- diagnose equipment, communication or software issues;
- provide technical support;
- maintain the reliability, security and performance of our systems;
- understand how our products and services are being used;
- improve existing Smithtek products and services;
- develop and test new functionality;
- investigate faults, misuse or security incidents; and
- comply with applicable legal or regulatory requirements.

Smithtek will not use customer-specific Operational Data for an unrelated purpose unless authorised by the customer or otherwise permitted or required by law.

4. Ownership of your data

As between you and Smithtek, you retain your rights and interests in the Operational Data that you or your equipment provide to Smithtek.

Smithtek does not claim ownership of your Operational Data simply because it is transmitted through or stored on a Smithtek system.

Where Operational Data originates from third-party equipment, systems or data sources, ownership and use may also be subject to the terms of the relevant third party.

You are responsible for ensuring that you have the necessary rights or authority to provide data to Smithtek where that data relates to another person, organisation, property or system.

5. Permission to use your data to provide the service

To provide our products and services, you authorise Smithtek to host, store, transmit, process, reproduce, display and otherwise use Operational Data to the extent reasonably necessary to provide and support the services you use.

This may include allowing Smithtek to:

- receive data from connected equipment;
- store data using Smithtek or third-party infrastructure;
- process data for dashboards, calculations, alarms and automation;
- transmit data between authorised devices and services;
- back up and restore data;
- diagnose or correct errors;
- provide technical support; and

- share data with persons or systems authorised by you.

This permission applies only for the purposes described in this Policy, our Privacy Policy, the relevant service agreement or as otherwise authorised by you.

6. Aggregated and de-identified data

Smithtek may use aggregated or de-identified information to understand system performance, improve our products and services, identify technical trends and assist with product development.

Where we use information in this way, we will take reasonable steps to ensure that it does not identify an individual customer, user or site.

Smithtek does not sell customer-specific Operational Data to third parties for their own commercial or marketing purposes without the customer's express authorisation.

7. Sharing Operational Data

Smithtek may provide access to Operational Data where necessary to operate or support our products and services. This may include:

- cloud hosting and data storage providers;
- telecommunications and network providers;
- email and SMS notification providers;
- satellite or communications providers;
- software and technology providers;
- technical support providers;
- contractors, installers and integration partners where required for the relevant project;
- persons or organisations authorised by you; and
- government agencies, regulators or other parties where disclosure is required or authorised by law.

Service providers are given access only to the information reasonably required for the services they provide.

Smithtek does not sell customer-specific Operational Data to third parties for their independent commercial use without your permission.

Where data is stored or processed outside Australia, the handling of personal information is also subject to the overseas handling provisions in our Privacy Policy.

8. Access by authorised users

Customers may permit other users to access their Operational Data, including employees, contractors, technicians, consultants or other authorised persons.

The level of access available to a user may depend on their assigned permissions or role.

Customers are responsible for deciding who should have access to their systems and for removing access when it is no longer required.

Smithtek may also access Operational Data where reasonably necessary to provide technical support, investigate faults, maintain systems, respond to security incidents or otherwise provide the requested services.

9. Data security

Smithtek takes reasonable technical and organisational measures to protect Operational Data against unauthorised access, loss, misuse, interference or disclosure.

Depending on the service being used, these measures may include access controls, user permissions, authentication, system monitoring, backups and security controls implemented by our technology and hosting providers.

No internet, communications or electronic storage system can be guaranteed to be completely secure. Customers should also take appropriate precautions to protect their equipment, user accounts, passwords, networks and connected systems.

10. Customer responsibilities

You are responsible for:

- keeping usernames, passwords and other account credentials secure;
- ensuring access is only provided to authorised users;
- maintaining appropriate security for equipment and networks under your control;
- notifying Smithtek if you become aware of unauthorised access or a security issue;
- ensuring information supplied to Smithtek is lawful and accurate where reasonably practicable; and
- ensuring you have permission to collect or transmit data from equipment, sites or third parties connected to the service.

11. Data retention

Smithtek retains Operational Data for as long as reasonably required to provide the relevant service, meet contractual requirements, maintain system functionality and comply with applicable legal obligations.

Retention periods may vary depending on the Smithtek product, service, subscription or storage arrangement being used.

Historical data may be automatically removed or overwritten after the applicable retention period.

Backup copies may remain for a limited period after data has been deleted from the active system.

Where a specific retention period forms part of a service plan or agreement, that period will apply to the relevant service.

12. Data access and portability

Where supported by the relevant service, customers may access, view or export their Operational Data using available dashboards, reports, APIs or export tools.

If you require Operational Data in a form that is not available through the service, you may contact Smithtek. We will consider reasonable requests subject to technical capability, security, contractual obligations and applicable law.

In some circumstances, data may not be available in its original format or may require processing before it can be provided.

13. Deletion of data

Customers may request deletion of Operational Data associated with their account or service.

Smithtek will action reasonable deletion requests where technically practicable and subject to any legal, contractual, security, backup or record-keeping requirements.

Deleting Operational Data may affect the operation of dashboards, reports, alarms, historical trends or other services that rely on that information.

Information that has already been securely aggregated or de-identified so that it can no longer reasonably be associated with the customer, individual or site may not be capable of being removed from aggregated datasets.

14. When a service or account ends

If your Smithtek service or subscription ends, access to associated Operational Data may also end.

Customers should export any information they require before terminating a service where export functionality is available.

Smithtek may retain information for a reasonable period following termination to allow for account administration, recovery, backups, legal obligations or resolution of disputes. Data may subsequently be deleted or de-identified in accordance with this Policy and our normal data retention practices.

15. Data breaches and security incidents

If Smithtek becomes aware of a security incident affecting Operational Data, we will investigate the incident and take reasonable steps to contain and remediate it.

Where an incident involves personal information, Smithtek will also assess and respond to the incident in accordance with our Privacy Policy and any applicable legal obligations, including notification requirements where applicable.

16. Business transfers

If Smithtek undergoes a merger, acquisition, restructuring, sale of business or transfer of assets, Operational Data may form part of the assets or services transferred.

Where this occurs, Smithtek will take reasonable steps to ensure that Operational Data continues to be handled in accordance with applicable contractual and legal obligations.

Where appropriate, affected customers will be notified of material changes to how their data will be handled.

17. Third-party products and integrations

Smithtek products and services may connect to equipment, software, networks or services provided by third parties.

Information sent to or received from those services may also be subject to the third party's terms, privacy policy or data use practices.

Smithtek is not responsible for the independent data handling practices of third parties where those parties operate outside Smithtek's control.

18. Changes to this Policy

Smithtek may update this Data Use Policy from time to time to reflect changes to our products, services, technology, business practices or legal requirements.

The current version will be made available through our website.

Where we make a material change that significantly affects how customer Operational Data is handled, we may provide additional notice where appropriate.

19. Contact us

If you have questions about this Data Use Policy or how Smithtek handles Operational Data, please contact us:

Smithtek Pty Ltd
Unit 2/13 Mackinnon Street
Rockingham WA 6168
Australia
Phone: (08) 6118 9176
Email: info@smithtek.com.au
Website: www.smithtek.com.au