

Tailspin Service Terms

Tailspin Service Terms (version 2026.3, last updated 1 August 2026). Printed from the web on 28 September 2026 from <https://tailspin-cloud.example/legal/service-terms>.

1. Scope. These Tailspin Service Terms are Online Terms for the Services made available by Tailspin Cloud Services Pte. Ltd. They apply to Customer's access to and use of Tailspin managed cloud, database, observability, support, portal, API, documentation and related service features. These Service Terms supplement the Agreement and each Order Form. If an Order Form identifies a specific Service, these Service Terms apply to that Service unless the Order Form expressly excludes them.

1.2 These Service Terms are written for standard cloud services used by business customers. They do not create a dedicated environment, bespoke security control, professional service deliverable, development commitment or regulatory undertaking unless the applicable Order Form says so. Capitalised terms not defined here have the meanings given in the Agreement. Service-specific attachments, support policies, acceptable use materials, subprocessor lists, security summaries and documentation pages may provide additional operational details for particular Services.

2. Accounts and administration. Customer is responsible for all activity under its accounts, API keys, tokens, identity integrations and administrator roles. Customer must keep account information current, protect credentials, configure appropriate access controls, and promptly disable access for users who no longer require the Services. Provider may rely on instructions submitted through authenticated accounts as Customer instructions.

2.2 Customer must ensure that its users comply with the Agreement, Documentation, Acceptable Use Policy and these Service Terms. Customer is responsible for Customer Content, configuration choices, retention settings, firewall rules, identity provider settings, integration endpoints, data mapping, workflow approvals and business decisions made through the Services. Customer must maintain current administrator contacts and emergency contacts in the customer portal.

3. Acceptable use. Customer must not use the Services to send unlawful, harmful, deceptive or infringing content; interfere with the integrity or security of the Services; probe or scan systems without authorisation; introduce malware; attempt to bypass usage limits; scrape or harvest data in violation of Law; or use the Services to operate critical safety systems where failure could lead to death, personal injury or severe environmental damage.

3.2 Provider may investigate suspected misuse and may remove or disable access to Customer Content or accounts where Provider reasonably believes action is necessary to protect the Services, comply with Law, or prevent harm to Provider, customers, users or third parties. Suspension and restoration are addressed in the Agreement. Customer must cooperate with Provider's investigation of misuse, including by preserving logs and identifying affected users where reasonably requested.

4. Service descriptions and documentation. Provider may publish Documentation, service descriptions, product guides, API references, release notes, security summaries and operational materials for the Services. Customer is responsible for reviewing applicable Documentation and using the Services in accordance with supported configurations, limits and instructions. Documentation is intended to describe operation of the Services and is not a legal warranty unless expressly incorporated into an Order Form.

4.2 Provider may make changes to the Services from time to time, including changes to features, user interfaces, APIs, dependencies, regions, limits and operational procedures. Provider will not materially decrease the core functionality of a generally available paid Service during the then-current Subscription Term, except where necessary for security, legal compliance, third-party dependency changes, end-of-life components or urgent operational reasons. Provider may provide notices of material changes through release notes, the customer portal or email.

5. Beta features. Provider may offer alpha, beta, preview, pilot, experimental or early access features. Beta features are provided as-is, may be modified or discontinued at any time, may be subject to additional limits, may not be covered by Service Levels, and should not be used for production workloads unless Provider expressly states otherwise. Customer uses beta features at its own risk.

5.2 Customer feedback about beta features may be used by Provider without restriction to improve the Services, develop roadmaps, fix defects, create documentation and evaluate market demand. Provider is not obligated to make any beta feature generally available or to preserve data stored only in a beta feature. Provider may require separate enablement, additional authentication, additional terms or technical prerequisites before Customer accesses beta features.

6. Third-party components. The Services may include, connect to or interoperate with third-party software, open source components, marketplaces, APIs, telecommunications networks, public internet

services, certificate authorities, registries, email relays, observability tools and customer-selected integrations. Provider is not responsible for third-party services outside Provider's control, even if the Services interoperate with them or Provider provides configuration guidance.

6.2 Open source components included in the Services are licensed under their applicable open source licences. To the extent an open source licence requires terms that are inconsistent with these Service Terms, the open source licence controls for that component only. Customer must obtain its own licences for third-party software or services that Customer chooses to connect to the Services. Provider may update or replace components for security, supportability or performance reasons.

7. Data and AI. This section describes certain data rights and operational uses that apply in addition to the DPA where applicable. Customer retains ownership of Customer Content. Provider may host, copy, transmit, cache, index, transform and display Customer Content as necessary to provide, secure, support, troubleshoot and operate the Services, comply with Law, enforce the Agreement, and protect the Services and users.

7.1 Usage Data. Provider may collect Usage Data about configuration, consumption, performance, capacity, errors, telemetry, user activity, feature use, API calls, support interactions, device and browser attributes, approximate location derived from IP address, and operational events. Provider may use Usage Data to administer accounts, calculate fees, monitor availability, improve reliability, plan capacity, prevent abuse, provide support and develop service analytics.

7.2 Aggregated statistics. Provider may create aggregated or de-identified statistics from Customer Content, Usage Data and operational records, provided the statistics do not identify Customer or any individual. Provider may use and disclose those statistics for benchmarking, security research, product planning, marketing, reporting, financial analysis and service improvement. Aggregated statistics may be retained after termination of the Agreement.

7.3 Provider may use Customer Content and Usage Data to develop, train, test and improve its products, services and machine learning models. Provider applies internal controls designed to reduce unauthorised disclosure of Customer Content during such activities, but Customer is responsible for ensuring that Customer's submission of Customer Content to the Services is permitted for these purposes.

7.4 Customer may configure available retention, deletion, logging and export settings. Provider may retain copies of Customer Content in backups, logs, caches and security records for limited periods in accordance with standard retention practices. Deletion from active systems does not immediately remove all copies from backup or disaster recovery media. Customer should use available export tools before deleting content or terminating Services.

8. Support policy. Provider provides support through the customer portal, support email and other channels described in the Documentation or Order Form. Support covers incidents, configuration questions, billing routing, service requests and reasonable troubleshooting for supported Services. Provider may require Customer to provide logs, screenshots, timestamps, affected user details, reproduction steps and approval for changes.

8.2 Support does not include development of Customer applications, custom code review, end-user training, data cleansing, correction of Customer Content, third-party product administration, on-site support, or work outside supported configurations unless purchased as Professional Services. Provider may close tickets that are inactive, duplicated, resolved, outside scope or awaiting Customer information for an extended period. Response targets, if any, are stated in the applicable service level schedule or support plan.

9. Security and operational practices. Provider maintains administrative, technical and physical safeguards designed to protect the Services. Customer remains responsible for endpoint security, user access, identity provider controls, network connectivity, Customer Content, local backups, business continuity plans and compliance decisions. Security features must be configured by Customer where they are optional or tenant-specific.

9.2 Provider may monitor use of the Services for security, reliability, abuse prevention, capacity management and compliance with these Service Terms. Customer must not disable, interfere with or falsify monitoring, logging or metering mechanisms. Provider may throttle, rate limit or restrict traffic that threatens the integrity, security or availability of the Services. Provider may also block traffic from known malicious sources or unsupported clients.

10. Fees, metering and limits. Some Services are subject to usage limits, storage limits, retention limits, API limits, seat quantities, log ingestion limits, fair use thresholds or other entitlements. Provider may measure consumption using its systems. Usage beyond purchased quantities may be rejected, throttled, suspended or charged at the applicable rates in the Order Form, Documentation or then-current price list.

10.2 Customer is responsible for monitoring consumption and configuring alerts where available. Provider may provide dashboards or reports, but those materials are informational and do not amend invoice obligations. Free, trial or promotional credits may expire, may be subject to additional terms, and may be withdrawn if Customer violates the Agreement or these Service Terms. Provider may require an updated Order Form before enabling materially higher capacity.

11. Changes to these terms. Provider may update these Service Terms at any time by posting a revised version; the revised version applies from the date of posting. Provider may identify the version number and last updated date on the web page. Customer is responsible for reviewing the Service Terms periodically and ensuring that its use of the Services remains compliant.

11.2 Continued use of the Services after posting of revised Service Terms constitutes acceptance of the revised version. If Customer does not agree to a revised version, Customer must stop using the affected Services and may exercise any termination right expressly available under the Agreement. No purchase order, portal note, email footer or other Customer document modifies these Service Terms unless signed by Provider's authorised signatory.

12. General provisions. Provider may provide notices about these Service Terms through the website, customer portal, email, status page or Documentation. If any provision of these Service Terms is unenforceable, the remaining provisions remain in effect. Provider's failure to enforce a provision is not a waiver. Headings are for convenience only and do not affect interpretation.

12.2 These Service Terms are part of the Online Terms referenced in the Agreement. They do not amend an Order Form except as provided by the Agreement's order of precedence and online terms provisions. If Provider publishes translated or regional explanatory materials, the English version of these Service Terms controls unless the Agreement expressly states otherwise. Archived versions may be made available for reference but do not apply after a revised version is posted.

12.3 Customer should retain a copy of the version that applies on the date of signature for its own records. Provider's publication of examples, frequently asked questions, implementation guides or informal notes does not vary these Service Terms unless the material expressly states that it is a binding addendum issued by Provider's legal department.