Rapport Product Terms

Product Terms under the Rezolve.ai Master Terms

These Rapport Product Terms (the "**Rapport Terms**") are Product Terms under the Rezolve.ai Master Terms (the "**Master Terms**") between Actionable Science, Inc., a Delaware corporation ("**ASC**"), and the customer that subscribes to Rapport (the "**Customer**"). They form part of the Agreement only when the Customer subscribes to Rapport, whether by executing an Order Form or by Online Subscription. Capitalised terms not defined in these Rapport Terms have the meanings given in the Master Terms.

1. Scope and precedence

1.1 These Rapport Terms supplement the Master Terms for Rapport only. They do not apply to any other Service and do not alter the terms of any other Service.

1.2 If these Rapport Terms conflict with the Master Terms, these Rapport Terms prevail for Rapport. The Data Processing Addendum, including the Rapport Data Processing Annex (Annex R), prevails on matters concerning the Processing of Personal Data. An Order Form prevails only for a provision it expressly identifies as overriding these Rapport Terms.

1.3 Schedule A (Default Settings) and Schedule B (Supported Platforms and Network Requirements) form part of these Rapport Terms.

2. Definitions

2.1 "**Administrator**" means an Operator to whom the Customer has assigned an administrator role in the Rapport Console.

2.2 "**Agent**" means the Rapport software installed on Enrolled Devices, including the Linux Preview Agent, and all updates, patches and new releases that ASC makes available.

2.3 "**AI Features**" means the AI Assistant, copilot, script drafting, issue resolution, investigation, patch-risk assessment and any other Rapport feature that uses a large language model.

2.4 "**AI Assistant**" means the AI Feature that investigates an Enrolled Device by running Diagnostic Tools on it, explains its findings and proposes Device Actions.

2.5 "**Approval Controls**" means the Rapport mechanisms that require a Device Action to be approved, verified by multi-factor authentication or justified with a recorded reason before it runs.

2.6 "**Audit Log**" means the record in the Rapport Console of Operator activity, Device Actions, approvals, reasons, AI Feature tool calls and their results.

2.7 "**Device Action**" means any action that runs on, changes or retrieves content from an Enrolled Device, including commands, scripts, file transfers, software and patch deployments, service restarts, reboots, Agent updates and actions proposed by the AI Assistant.

2.8 "**Device Data**" means data collected from or about Enrolled Devices through Rapport, including telemetry, inventory, experience events, workforce activity aggregates and the output of Device Actions. Device Data is Customer Data.

2.9 "**Diagnostic Tools**" means the native checks, file metadata collection and shell commands the Agent can run to gather information about an Enrolled Device.

2.10 "**Enrolled Device**" means a computer on which the Agent is installed and enrolled to the Customer's Rapport tenant using an Enrollment Token.

2.11 "**Enrollment Token**" means a tenant-specific, expiring and use-limited credential issued in the Rapport Console to enrol devices.

2.12 "**Linux Preview Agent**" means the version of the Agent for Linux designated by ASC as a preview.

2.13 "**Operator**" means a User whom the Customer authorises to access the Rapport Console.

2.14 "**Rapport**" means ASC's device experience and support Service, comprising the Rapport Console, the Agent, the AI Features, the Rapport gateway and back-end services, application programming interfaces and the related Documentation.

2.15 "**Rapport Console**" means the web application through which Operators access Rapport.

2.16 "**Service Data**" means technical data about the operation of Rapport and the Agent (such as Agent version, health counters, error codes, latency and usage volumes), which may include device identifiers, account identifiers and IP addresses but does not include the content of Device Data.

2.17 "**Workforce Activity**" means the optional Rapport module that measures active, idle, after-hours and weekend time and foreground time by broad application category on Enrolled Devices.

3. Subscription and accounts

3.1 **Online Subscription.** By creating a Rapport tenant and accepting these Rapport Terms online, the person accepting represents that they are authorised to bind the Customer, and the Customer accepts the Master Terms, these Rapport Terms and the Data Processing Addendum. ASC records the identity of the person accepting, the time of acceptance and the version of each document accepted. The Master Terms, these Rapport Terms and the Data Processing Addendum will be made available to the Customer before acceptance, in a form that the Customer can download and retain.

3.2 **Plans.** Rapport is offered on the plans ASC makes available from time to time. New tenants start on the free plan. Paid plans, usage limits, fees and any service levels are set out in an Order Form.

3.3 **Operators.** The Customer is responsible for all activity under its Operators' accounts. Operators must be at least 18 years old, authorised by the Customer and, where they are not the Customer's employees, bound by confidentiality obligations to the Customer. The Customer must keep multi-factor authentication enabled for every Operator and must promptly remove or downgrade access that is no longer required.

3.4 **Enrollment Tokens and credentials.** The Customer must keep Enrollment Tokens, API keys and device credentials confidential, distribute them only through secure channels, and revoke them in the Rapport Console without delay if they may have been exposed. Revoking an Enrollment Token stops further enrolment but does not disconnect devices already enrolled.

4. Licence to the Agent

4.1 **Grant.** Subject to the Agreement and payment of any applicable fees, ASC grants the Customer a non-exclusive, non-transferable, non-sublicensable, revocable licence during the Subscription Term to install and run the Agent, in object-code form only, on devices that the Customer owns or is authorised to manage, solely to use Rapport for the Customer's internal business purposes and in accordance with the Documentation. The Customer may permit its service providers to install the Agent on its behalf, and remains responsible for their acts and omissions.

4.2 **Restrictions.** Sections 3 and 7.2 of the Master Terms apply to the Agent. In addition, the Customer must not: (a) modify, patch or tamper with the Agent or its configuration other than through the Rapport Console; (b) remove or alter any notice, signature or integrity mechanism; (c) use the Agent with any service other than Rapport; (d) interfere with the Agent's command classification, Approval Controls, audit logging or update mechanism; or (e) distribute the Agent to any third party except as permitted in Section 4.1.

4.3 **Releases and updates.** ASC may release updates to the Agent to provide features, fixes and security improvements. The Customer controls the adoption of Agent releases on its devices through the release settings in the Rapport Console (individual approval, automatic adoption or hold). A hold prevents future update attempts but does not stop an installation already in progress, and does not affect packages the Customer deploys through its own device-management tools. ASC supports the current release and the immediately preceding release of the Agent. ASC may require the Customer to adopt a release that fixes a security vulnerability within a reasonable period stated in a notice.

4.4 **Integrity.** ASC code-signs Windows (MSI) and macOS (PKG) releases of the Agent and signs Agent policies issued by Rapport. The Customer must install the Agent only from packages or install commands obtained from the Rapport Console or from ASC, and must not disable signature or certificate verification.

4.5 **Linux Preview Agent.** The Linux Preview Agent is provided as a preview under the Trial Version terms in Section 2.2 of the Master Terms. It is installed by script, has no installer package, **is verified by signature and checksum during installation**, and may change or be withdrawn without notice. Sections 6 (Security and Data) of the Master Terms and the Data Processing Addendum continue to apply to Device Data collected by it.

4.6 **Third-party software.** The Agent and the Rapport Console include open-source software listed in the Rapport Open-Source Notices, each licensed under its own terms. Those terms govern the open-source software, and nothing in the Agreement restricts rights granted under them.

4.7 **Uninstallation.** On expiry or termination of the Subscription Term, or on retirement of a device, the Customer must uninstall the Agent from the affected devices. The Customer may retire and erase an Enrolled Device in the Rapport Console, which revokes the device's credentials and deletes its Device Data from Rapport in accordance with Section 10.6.

4.8 **Export and sanctions.** The Agent contains encryption technology and is subject to United States export control sanctions laws and other applicable export laws. The Customer must not export, re-export or install the Agent, or permit access to Rapport, in breach of those laws, including in or for a comprehensively sanctioned country or region, for a restricted party, or for a prohibited end use. Customer represents it is not on a US, EU, UK or UN restricted-party list (incl. SDN and Entity List) and further represents that no export to Russia or Belarus will be undertaken without any required licence.

5. Customer responsibilities

5.1 **Authorised devices.** The Customer may enrol only devices that it owns or is legally authorised to manage. A device owned by an individual may be enrolled only with that individual's prior informed consent, which the Customer must be able to demonstrate.

5.2 **Notice, lawful basis and consultation.** To the extent the Customer determines the purposes and means of processing Device Data, the Customer acts as controller or data fiduciary, as applicable, and is responsible for: (a) determining a lawful basis for its use of Rapport; (b) giving individuals, including employees and contractors, any notice required by law before their devices are enrolled or Workforce Activity is enabled; (c) obtaining any consent, and completing any consultation, works-council or similar process, required by law; and (d) carrying out any data protection impact assessment required by law. ASC provides an Employee Privacy Notice template for convenience; the Customer is responsible for adapting it and for its use. Nothing in this Section limits ASC's obligations under applicable data protection law or the Data Processing Addendum.

5.3 **Configuration.** The Customer determines which Rapport modules, Diagnostic Tools, Device Actions, AI Features and integrations are enabled, and which Operators may initiate or approve Device Actions. Schedule A sets out the defaults for new tenants. The Customer is responsible for any change it makes to those defaults, including any relaxation of Approval Controls.

5.4 **Privilege of the Agent.** The Customer acknowledges that the Agent runs as a privileged system service (SYSTEM on Windows; root on macOS and Linux) so that it can diagnose and remediate devices; that Device Actions can therefore read content on, and change the configuration of, Enrolled Devices; and that command classification, Approval Controls and output limits are safeguards and not an operating-system sandbox. The Customer must assign Device Action and approval permissions only to Operators it trusts, with the least privilege necessary.

5.5 **Review and testing.** Before approving a Device Action, the Operator must review the exact command, script or file path, its target devices and its likely effect. The Customer is responsible for testing scripts, patches and software before broad deployment, including by using staged rollouts and maintenance windows, and for maintaining backups of Enrolled Devices and data.

5.6 **Network.** The Customer is responsible for meeting the network requirements in Schedule B, including outbound connectivity and proxy and TLS-inspection configuration, for its devices.

5.7 **Restricted data.** The Customer must not use Rapport to deliberately collect or store payment card data, protected health information, government identification numbers, special categories of personal data (as defined in the GDPR) or sensitive personal data or information under Indian law (including passwords, financial information and health information), except to the extent such data is incidentally present in content that Operators access through Device Actions. A Customer that is a covered entity or business associate under HIPAA must not enrol devices that store or access protected health information. Rapport is not designed to meet sector-specific requirements (such as HIPAA or PCI DSS) and no business associate agreement is offered for Rapport. Any such data incidentally accessed remains subject to applicable law and the Data Processing Addendum. The Customer must configure access permissions and Device Actions to minimise access to data that is unnecessary for the authorised purpose.

6. Acceptable use

6.1 In addition to Section 3 of the Master Terms, the Customer must not, and must ensure that its Operators do not, use Rapport to:

(a) monitor any individual covertly, or in breach of any employment, privacy, electronic-monitoring, wiretapping or communications law;

(b) rate, rank or score the productivity, performance or behaviour of an individual, or make a decision about an individual's employment based solely on Rapport data;

(c) use the AI Features to evaluate, profile or make decisions about individuals;

(d) access an individual's personal accounts, private communications or personal files without a lawful and documented reason;

(e) enrol a device that the Customer does not own or is not authorised to manage;

(f) circumvent, disable or degrade command classification, Approval Controls, multi-factor authentication, audit logging or tenant isolation;

(g) deploy malicious code, conduct attacks against third parties, or disrupt systems or networks other than in the course of legitimate administration of the Customer's own systems; or

(h) probe, scan or test the security of Rapport other than in accordance with the Vulnerability Disclosure Policy.

6.2 ASC may suspend access to Rapport, to specific features, or to specific Operators if it reasonably believes that Rapport is being used in breach of this Section 6, or in a manner that threatens the security or integrity of Rapport, Enrolled Devices or other customers. ASC will give notice and an opportunity to cure where practicable, and will limit the suspension to what is reasonably necessary.

7. Device Actions and controls

7.1 **Initiation.** Device Actions run only when initiated by an Operator, approved through Approval Controls, or triggered by a rule or schedule that the Customer has configured and approved. Rapport and the AI Features propose Device Actions. However, commands classified as read-only may run without separate approval where permitted by the Customer’s settings, as described in Section 7.3. ASC support personnel initiate a Device Action only on the Customer’s written instruction for a specific support case, as described in the Rapport Support Policy.

7.2 **Approval.** For new tenants, each script and file transfer must be approved before it runs: (a) by a second Operator with approval rights; or (b) where the Customer has only one Administrator, by that Administrator after entering a written reason. File actions also require a fresh multi-factor authentication check. Rules, scheduled checks and requests initiated by a machine always require approval.

7.3 **AI Assistant commands.** The Agent classifies each shell command requested through the AI Assistant on the device before running it, independently of the AI model. Commands classified as read-only may run automatically where the Customer's settings permit. Commands that modify a device or require elevated privileges are held for approval, and approval applies only to the individual command approved. Commands classified as destructive or disallowed are refused. The AI Assistant cannot read operating-system credential stores and, on Enrolled Devices running Agent version 1.1 or later, cannot read browser, email or messaging data stores (including those of Outlook, Microsoft Teams and Slack). Commands that read the clipboard or capture the screen are held for approval; if approved, the content they return passes through the same data loss prevention filtering and is sent to Anthropic with the other results.

7.4 **Records.** Rapport records every Device Action request, approval, reason, multi-factor check, execution result and AI Feature tool call in the Audit Log.

7.5 **Limits of safeguards.** Command classification and Approval Controls reduce risk but may not identify every effect of a command, script or deployment. A completed Device Action is not confirmation that an underlying issue is resolved.

7.6 **Responsibility for Device Actions.** Subject to Section 12 of the Master Terms, ASC is not responsible for any loss, damage, data loss, service interruption or configuration change resulting from a Device Action that an Operator initiated or approved, or that ran automatically under settings, rules or schedules enabled or configured by the Customer, including read-only commands permitted under Section 7.3, except to the extent caused by ASC's breach of the Agreement or a defect in Rapport that caused the Device Action to behave materially differently from its description in the Documentation.

8. AI Features

8.1 **Enablement.** AI Features are disabled for new tenants until an Administrator enables them. A single tenant setting enables or disables all AI Features. On enablement, Rapport identifies the AI provider and the data that

AI Features send to it, including whether file metadata collection and read-only Commands may run without separate approval and records who enabled them and when.

8.2 **Provider.** AI Features use large language models provided by Anthropic. ASC's agreement with Anthropic provides that inputs and outputs are not retained by Anthropic after processing and are not used to train Anthropic's models. Anthropic is listed in the Sub-processor List.

8.3 **Data sent.** When AI Features are enabled, Rapport sends the Operator's prompts, conversation context, tool definitions, relevant device facts and the results of Diagnostic Tools (which may include file metadata such as names, paths and sizes, and command output; the AI Assistant does not read the contents of files) to the AI provider through the Rapport gateway. Rapport applies automated data loss prevention filtering, including masking of text matching credential patterns, before sending it, on a best-effort basis. Provider credentials are held server-side and are not exposed to Enrolled Devices or browsers.

8.4 **Account. All AI Features use ASC's Anthropic account; customer-supplied API keys are not supported. ASC remains responsible as processor for this processing.**

8.5 **Output.** AI output is generated probabilistically and may be inaccurate, incomplete or unsuitable. Confidence levels are aids to review and are not guarantees. The Customer's Operators must review AI findings and proposed Device Actions before relying on or approving them, and must not use AI output as the sole basis for any decision with legal or similarly significant effects on an individual.

8.6 **Untrusted content.** Content on Enrolled Devices may contain text that attempts to influence the AI Features. Device-side command classification and Approval Controls operate independently of the AI model to limit the effect of such content.

8.7 **No training.** ASC does not use Customer Data, including Device Data, prompts and AI outputs, to train or fine-tune AI models.

9. Integrations

9.1 The Customer may connect Rapport to third-party systems it chooses, such as IT service management platforms, collaboration tools and webhooks ("**Customer Integrations**"). Customer Integrations act on the Customer's instructions, are not ASC sub-processors, and are governed by the Customer's agreements with their providers. ASC transmits Customer Data to a Customer Integration only as the Customer configures.

9.2 Public API and Model Context Protocol (MCP) access are disabled for new tenants. An Administrator may enable them after a fresh multi-factor authentication check and a stated reason, which Rapport records. The Customer is responsible for API keys it issues and for the systems that use them.

10. Data

10.1 **Ownership.** As between the parties, the Customer owns Device Data. ASC processes Device Data only to provide, secure, support and improve the operation of Rapport for the Customer, in accordance with the Data Processing Addendum.

10.2 **Service Data.** ASC may collect and use Service Data to operate, secure, support and improve Rapport. Service Data is Analytical Data under Section 6.6 of the Master Terms. To the extent Service Data is personal data, ASC processes it as a controller in accordance with its Privacy Policy, limits it to what is required and uses it in de-identified, anonymised, or aggregated form, where possible. Device Data, including the content of Device Actions and AI conversations, is not Analytical Data.

10.3 **Routine monitoring.** Rapport's scheduled collection never captures keystrokes, screen content, clipboard contents, browsing history, the content of documents or messages, process arguments, file paths or wireless network names. Device Actions and AI Features, when used, can access device content as described in Sections 7 and 8.

10.4 **Workforce Activity.** Workforce Activity is disabled for new tenants. When enabled: application names are categorised on the device and do not leave it; results are displayed only for groups of at least five devices; and access to Workforce Activity reports requires a separate permission. Before enabling it, an Administrator must confirm that the Customer has given any required notice to affected individuals.

10.5 **Retention.** The Customer sets a retention period for each category of Device Data in the Rapport Console, between 1 and 3,650 days, except that the Audit Log is retained for at least 365 days. Rapport deletes data automatically when its retention period ends. Default periods are set out in Annex R of the Data Processing Addendum. The Customer must select retention periods appropriate to its purposes and applicable law.

Availability of a retention setting does not authorise retention beyond what is lawfully necessary. Deletion and any exceptions for backups or legally required retention are governed by the Data Processing Addendum.

10.6 **Device retirement.** When an Administrator retires and erases an Enrolled Device, Rapport revokes the device's credentials and deletes its Device Data, including its release-provenance and policy records. Audit Log entries relating to the device are retained for the Audit Log retention period.

10.7 **Location.** Rapport stores Customer Data in the United States. ASC will give notice under the Data Processing Addendum before changing the country in which Customer Data is stored. Authorised personnel of ASC's affiliate, Actionable Science Labs Private Limited in India, may access Customer Data remotely where necessary to provide support, for a specific support case and with access logged, subject to the Data Processing Addendum. They do not store copies of Customer Data in India. Details of the hosting providers and other sub-processors are set out in the Sub-processor List.

10.8 **Export and deletion on exit.** Operators can export reports in CSV format at any time. On termination, Section 13.8 of the Data Processing Addendum governs the export and deletion of the Customer's Rapport data, and replaces Section 14.4(iii) of the Master Terms for Rapport.

11. Security

11.1 **ASC measures.** In addition to Section 6 of the Master Terms, ASC will maintain for Rapport: tenant isolation of Customer Data; multi-factor authentication for Operator sessions; outbound-only Agent connectivity over HTTPS with certificate verification; device-bound Agent credentials; signed Agent policies and code-signed Windows and macOS releases; server-side storage of AI provider credentials; and the Audit Log.

11.2 **Incidents.** ASC will notify the Customer of a Personal Data Breach affecting Rapport in accordance with Clause 10 of the Data Processing Addendum. If ASC becomes aware of a compromise of the Agent, its signing keys or its update channel, ASC will notify affected customers without undue delay, may suspend Agent updates or Device Actions to contain the incident, and will provide remediation instructions. Nothing in this section limits either party's mandatory incident-reporting obligations under applicable law. ASC will provide information reasonably available to it that the Customer reasonably requires to meet its applicable reporting obligations.

11.3 **Customer measures.** The Customer is responsible for the security of its Enrolled Devices, its Operators' accounts and credentials, its Customer Integrations and its API keys, and for promptly revoking compromised credentials and devices.

11.4 **Certification status.** Rapport is operated under ASC's information security programme. ASC intends to bring Rapport within the scope of its SOC 2 Type II and ISO/IEC 27001 programme. Until a report or certificate expressly covers Rapport, ASC's existing reports and certificates do not cover Rapport.

12. Beta, preview and service levels

12.1 Rapport is currently offered as a beta. While a beta or a feature designated as preview (including the Linux Preview Agent) is provided free of charge, it is a Trial Version under Section 2.2 of the Master Terms: features may change or be withdrawn, and no service levels or service credits apply. Section 6 of the Master Terms, these Rapport Terms and the Data Processing Addendum continue to apply.

12.2 Service levels for paid plans, if any, are set out in the Order Form. Remote terminal is not available. If ASC later offers remote terminal, it will be off by default and enabled only by an Administrator after notice under Section 15.1.

12.3 Support is provided in accordance with the Rapport Support Policy.

13. Term and termination

13.1 Notwithstanding Section 2.2 of the Master Terms, a free-plan subscription continues until terminated. Either party may terminate a free-plan subscription for convenience on 30 days' written notice, and ASC may end the beta on 30 days' notice. Paid subscriptions continue for the Subscription Term in the Order Form.

13.2 On expiry or termination: (a) the licence in Section 4 ends and the Customer must uninstall the Agent; (b) Agents that remain installed will no longer be supported; and (c) Section 10.8 applies to the Customer's Rapport data.

14. Warranties, liability and indemnity

14.1 Sections 9, 10 and 12 of the Master Terms apply to Rapport. Without limiting them, ASC does not warrant that Rapport will detect every issue on a device, that AI output or any proposed Device Action will be correct, or that any Device Action will achieve its intended result.

14.2 Nothing in these Rapport Terms extends ASC's aggregate liability beyond the limit in Section 12.1 of the Master Terms.

14.3 In addition to Section 13.2 of the Master Terms, the Customer will defend, indemnify and hold harmless ASC against third-party claims, including claims by the Customer's employees, arising from: (a) the Customer's enrolment of devices it was not authorised to manage; (b) the Customer's failure to give notice, obtain consent or complete consultation required by law under Section 5.2; or (c) Device Actions or uses of Rapport in breach of Section 6. This indemnity includes reasonable costs incurred by ASC in responding to related regulatory proceedings, and fines or penalties only to the extent recoverable from the Customer under applicable law.

15. General

15.1 **Changes.** ASC may update these Rapport Terms at least 30 days' notice, except where needed urgently for security, in which case notice will be given as soon as practicable. ASC may change default settings for new tenants at any time; changes to the settings of an existing tenant that materially reduce its protections require notice to the Customer.

15.2 **Survival.** Sections 4.7, 4.8, 7.6, 10, 13.2 and 14 survive termination.

Schedule A – Default settings for new tenants

Feature	Default	Who can change it
Routine collection (heartbeat, inventory, telemetry, experience)	On, as set by the signed collection policy	Administrator
Workforce Activity	Off	Administrator, after confirming notice to individuals
Scripts	Approval required before each run (second Operator, or lone Administrator with recorded reason)	Administrator
File transfer (pull and push within approved paths)	Approval required; fresh MFA check	Administrator
Rules, scheduled checks, machine-initiated requests	Approval always required	Not configurable
AI Features (all)	Off until enabled by an Administrator	Administrator
AI Assistant read-only checks	May run automatically once AI Features are enabled	Administrator
Public API and MCP access	Off	Administrator, with fresh MFA check and stated reason
Remote terminal	Not available	—
Agent releases	Individual approval required	Administrator

Schedule B – Supported platforms and network requirements

Platform	Supported versions	Installation
Windows	Supported Windows 11 releases; Windows 10 22H2 with active Extended Security Updates; Windows Server 2022 and later (x64). x64 and ARM64. Requires .NET Framework 4.7.2 or later	Code-signed MSI; administrator installation; runs as SYSTEM
macOS	macOS 14 and later with current Apple security updates; Intel and Apple silicon	Code-signed universal PKG; root installation; launchd system service
Linux (preview)	Ubuntu 22.04 LTS and later; Debian 12 and later; RHEL, Rocky Linux and AlmaLinux 9 and later; systemd-based; x64 and ARM64	Install script, verified by signature and checksum; runs as root; no installer package

Operating systems must receive vendor security updates. 32-bit, preview, beta, containerised and end-of-life operating systems are not supported.

Network. The Agent requires DNS and outbound HTTPS (TCP 443) from its service account to the Rapport endpoints ASC designates; no inbound port is required. PAC/WPAD discovery and integrated NTLM/Kerberos proxy authentication are not supported. Where TLS inspection is used, the inspecting certificate authority must be trusted in the system store used by the Agent; certificate verification must remain enabled.