

Redesign Technology Terms

Version Date: September 2026

These Redesign Technology Terms (these "Technology Terms") supplement and are incorporated into the applicable agreement between The Drala Project, Inc. d/b/a The Redesign Group ("Redesign") and Customer, including Redesign's Services Terms and Conditions, Product Sales Terms and Conditions, Third-Party Services Terms and Conditions, Data Processing Agreement, applicable Order Form, Statement of Work, quote, product addendum, and any written master agreement between Customer and Redesign that applies to any Redesign Product or Redesign Application (collectively, the "Agreement").

These Technology Terms govern Customer's access to and use of Redesign Products and Redesign Applications, whether accessed through the Unified Portal, deployed within Customer's environment, delivered as hosted or cloud-based services, or provided in any other configuration. The main body of these Technology Terms governs product-wide functionality, including licensing, data, connectors, security, support, restrictions, suspension, disclaimers, and liability. The Addendums govern product-specific functionality only for the applicable Redesign Product or Redesign Application.

Capitalized terms used but not defined in these Technology Terms have the meanings given in the Agreement.

1. Definitions

1.1 "Addendum" means a product-specific or feature-specific addendum attached to or incorporated into these Technology Terms.

1.2 "Administrator" means an Authorized User designated by Customer or Redesign to administer Customer's account, organization, users, entitlements, permissions, configurations, integrations, workflows, or related settings.

1.3 "Authorized User" means any employee, contractor, consultant, administrator, agent, or other individual authorized by Customer or Redesign to access a Redesign Product or Redesign Application on Customer's behalf.

1.4 "Claim" means any civil, criminal, administrative, regulatory, arbitral, or investigative action, claim, demand, proceeding, or allegation brought or threatened by a third party.

1.5 "Connector" means any API, integration, agent, credential, plug-in, data connector, workflow, script, service account, software component, or other mechanism used to connect a Redesign Product or Redesign Application to Customer Systems, Third-Party Services, models, tools, applications, data sources, or environments.

1.6 "Customer Data" means data, content, files, documents, prompts, queries, inputs, outputs, records, information, metadata, logs, reports, credentials, configurations, system information, compliance evidence, Asset Data, and other materials submitted to, uploaded to, processed by, generated through, transmitted through, indexed by, analyzed by, or made available to Redesign by or on behalf of Customer in connection with the Redesign Products, Redesign Applications, or any related Redesign services or offerings.

1.7 "Customer Systems" means systems, networks, applications, environments, file systems, endpoints, infrastructure, databases, cloud environments, ERP systems, MES systems, operational technology systems, manufacturing systems, data repositories, and other technology assets owned, operated, controlled, or made available by or on behalf of Customer.

1.8 "Documentation" means Redesign's then-current technical documentation, user guides, administrative guides, deployment materials, release notes, product descriptions, support materials, and usage instructions applicable to the Redesign Products, Redesign Applications, or any related functionality.

1.9 "DPA" means Redesign's Data Processing Agreement applicable to Redesign's processing of Personal Data on behalf of Customer.

1.10 "High-Risk Use" means use in or for systems or activities where failure could reasonably result in death, serious bodily injury, severe physical damage, severe environmental damage, or other material harm requiring fail-safe performance.

1.11 "Losses" means damages, liabilities, losses, judgments, settlements, penalties, fines, costs, and expenses, including reasonable attorneys' fees.

1.12 "Output" means data, reports, summaries, analyses, responses, recommendations, control mappings, extracted information, workflows, automations, generated content, Asset Data, Lifecycle Recommendations, or other materials generated by or through a Redesign Product or Redesign Application.

1.13 "Personal Data" has the meaning given in the DPA.

redesign

1.14 "Provider Technology" means Redesign-owned or Redesign-licensed tools, software, scripts, utilities, agents, models, methodologies, processes, templates, configurations, and other technology used to provide Redesign Products or Redesign Applications.

1.15 "Redesign Application" means any Redesign product, platform, application, tool, software, workflow, module, or service made available by Redesign, including the Unified Portal, OpenCloud, Redesign Cloud Hosting Services, Redesign Exchange, Redesign C7e Enterprise AI Platform, Redesign AI Chat, Redesign GRC, C7e Studio, Asset Management Functionality, Marketplace Functionality, and any other application or module made available by Redesign from time to time.

1.16 "Redesign Configurations" means configurations, scripts, templates, workflows, automations, prompts, settings, and similar technical work product implemented or made available by Redesign.

1.17 "Redesign Product" means any proprietary Redesign software, subscription, application, platform, module, tool, or other Redesign-owned product made available to Customer under an applicable Order, excluding Third-Party Services.

1.18 "Security Breach" has the meaning given in the DPA. If the DPA does not apply, "Security Breach" means unauthorized access to or disclosure of Customer Data in Redesign's possession, custody, or control.

1.19 "Sensitive Data" has the meaning given in the DPA.

1.20 "Third-Party Services" means third-party products, models, tools, services, software, platforms, data sources, APIs, integrations, cloud services, hardware, software-as-a-service offerings, subscriptions, support, maintenance, service entitlements, or other services or offerings not owned or controlled by Redesign.

2. License and Entitlements

2.1 License Grant. Subject to Customer's payment of all applicable fees and compliance with the Agreement, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use the Redesign Products and Redesign Applications identified in the applicable Order solely for Customer's internal business purposes.

2.2 Entitlements. Customer may access only the Redesign Products, Redesign Applications, features, modules, environments, models, tools, workflows, Connectors, datasets, and entitlements included in the applicable Order or otherwise enabled by Redesign in writing. Portal visibility, catalog visibility, technical availability, beta access, trial access, or configuration access does not expand Customer's license, subscription scope, usage rights, support rights, service levels, procurement rights, or entitlements.

2.3 Application Addendums. Each Addendum applies only if the applicable Redesign Product or Redesign Application is identified in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer. Product-specific rights, restrictions, service descriptions, warranties, disclaimers, support commitments, usage limits, commercial terms, and termination effects are governed by the applicable Addendum.

2.4 No Implied Rights. Customer receives no ownership interest in the Redesign Products, Redesign Applications, Provider Technology, Redesign Configurations, Documentation, workflows, templates, scripts, models, software, APIs, interfaces, or Redesign intellectual property. All rights not expressly granted are reserved by Redesign and its licensors.

3. Deployment Models

3.1 Deployment Flexibility. Redesign Products and Redesign Applications may be accessed through the Unified Portal, deployed within Customer's environment, delivered as hosted or cloud-based services, deployed on-premises, or provided in any other configuration described in the applicable Order, Addendum, or Documentation.

3.2 On-Premises and Customer-Hosted Deployments. Where a Redesign Product is deployed within Customer's own infrastructure, Customer's environment, or Customer's cloud tenant, and Redesign does not host, operate, or control the production instance: (a) Customer is solely responsible for the security, availability, performance, configuration, backups, data integrity, access controls, identity management, network security, patching, and compliance of Customer's environment; (b) Redesign's license to use Customer Data applies only to the extent Redesign actually receives or accesses such data in connection with support, troubleshooting, updates, or other services expressly agreed in an applicable Order or SOW; (c) the DPA applies only to the extent Redesign processes Personal Data on behalf of Customer; and (d) Redesign is not responsible for Customer Data processed entirely within Customer's environment that is not transmitted to, accessed by, hosted by, or stored by Redesign.

redesign

3.3 Portal-Based Access. Where Customer accesses Redesign Products or Redesign Applications through the Unified Portal, the Unified Portal Addendum (Addendum A) applies.

3.4 Redesign-Hosted Cloud Services. Where Redesign hosts and operates infrastructure-as-a-service, platform-as-a-service, or software-as-a-service offerings, the Redesign Cloud Hosting Services Addendum (Addendum G) applies.

4. Accounts, Identity, and Administration

4.1 Account Registration. Customer and Authorized Users may be required to create accounts or use Redesign-approved identity credentials to access Redesign Products or Redesign Applications. Customer will ensure that all registration, account, and user information is accurate and kept current.

4.2 Administrators. Customer is responsible for designating and managing Administrators. Administrators may control Authorized User access, assign permissions, configure entitlements, view usage, access Customer Data, manage integrations, and take other administrative actions within the Redesign Products and Redesign Applications.

4.3 Organizational Accounts. If an Authorized User creates or accesses an account using an email address owned or controlled by Customer, Redesign may associate that account with Customer's organizational account. Customer acknowledges that Customer's Administrators may control such account, including access to Customer Data and usage history associated with that account.

4.4 Credential Security. Customer is responsible for maintaining the confidentiality and security of all credentials, accounts, tokens, keys, service accounts, SSO configurations, Administrator permissions, purchasing permissions, approval permissions, and access controls used by Customer or Authorized Users.

4.5 User Responsibility. Customer is responsible for all acts and omissions of Authorized Users and for all activity occurring under Customer's accounts, credentials, Connectors, procurement workflows, or environments, whether authorized by Customer or resulting from Customer's failure to maintain appropriate access controls.

4.6 Access Controls. Customer will maintain appropriate access controls for the Redesign Products and Redesign Applications, including unique user accounts, multi-factor authentication for privileged access, timely access removal for departed personnel, least-privilege permissions, and monitoring appropriate to Customer's risk profile.

5. Customer Responsibilities

5.1 Customer Systems. Customer is responsible for Customer Systems, including security, availability, performance, configuration, backups, data integrity, licensing, user access, permissions, change management, regulatory requirements, and all dependencies required for Redesign to provide the Redesign Products and Redesign Applications.

5.2 Customer Data. Customer is responsible for the accuracy, quality, legality, integrity, and appropriateness of Customer Data. Customer represents and warrants that it has all rights, consents, permissions, notices, and legal bases required to provide Customer Data to Redesign and to authorize Redesign to process Customer Data under the Agreement.

5.3 Cooperation. Customer will provide timely access, information, approvals, personnel, credentials, technical details, system documentation, procurement information, asset information, and other cooperation reasonably required for Redesign to provide the Redesign Products, Redesign Applications, and related services.

5.4 Critical Systems. Customer must identify in writing any critical production systems, including ERP, MES, manufacturing, operational technology, safety-related, regulated, or business-critical systems, before authorizing Redesign to connect to, ingest from, index, scan, analyze, or transfer data from such systems.

5.5 Backups. Unless expressly included in an applicable Order, Customer is responsible for backups, backup testing, restoration, business continuity, disaster recovery, and reconstruction of Customer Data and Customer Systems.

5.6 No Sensitive Data by Default. Customer will not submit, upload, grant access to, or otherwise make available Sensitive Data to any Redesign Product or Redesign Application unless the applicable Order expressly identifies the categories of Sensitive Data and any additional safeguards required for such processing.

6. Customer Data and Processing

6.1 Customer Ownership. As between Redesign and Customer, Customer retains all right, title, and interest in and to Customer Data.

6.2 License to Redesign. Customer grants Redesign a non-exclusive, worldwide, sublicensable, royalty-free license to host, access, use, process, copy, transmit, index, analyze, transform, display, route, store, retrieve, and otherwise process Customer Data as necessary to provide, secure, support, maintain, administer, improve, and troubleshoot the Redesign Products and Redesign

redesign

Applications; administer entitlements; provide support; operate Connectors; generate Output; perform workflows; comply with the Agreement and applicable Law; and enforce Redesign's rights. For on-premises and customer-hosted deployments, this license applies only to the extent Redesign actually receives or accesses Customer Data. For clarity, Redesign's right to improve Redesign Products and Redesign Applications does not include training or fine-tuning machine-learning or artificial-intelligence models using identifiable Customer Data except as permitted under Section 6.7.

6.3 Cross-Application Functionality. Where Customer uses multiple Redesign Products or Redesign Applications, Customer authorizes Redesign to process and make available Customer Data across enabled products and applications to provide cross-application workflows, reporting, search, indexing, insights, automation, security, entitlement management, asset management, marketplace, procurement, lifecycle, and administrative functionality.

6.4 Usage Data and Telemetry. Redesign may collect and use logs, metadata, usage data, performance data, diagnostic data, telemetry, entitlement data, and system information relating to Redesign Products and Redesign Applications to provide, secure, support, improve, and administer the Redesign Products and Redesign Applications, provided that Redesign will configure such measures in a manner designed to avoid collecting Customer workload content except as required to provide support, security, troubleshooting, or functionality requested by Customer.

6.5 Aggregated and De-Identified Data. Redesign may use aggregated, de-identified, or anonymized data that does not identify Customer or any individual for analytics, benchmarking, service improvement, security monitoring, product development, procurement insights, lifecycle planning, and similar business purposes.

6.6 Personal Data. To the extent Redesign processes Personal Data on behalf of Customer, the DPA applies. In the event of a conflict between these Technology Terms and the DPA with respect to the processing of Personal Data, the DPA controls.

6.7 AI Training and Improvement. Redesign and its Affiliates will not use identifiable Customer Data, including prompts, inputs, Output, or materials generated through AI-enabled functionality, to train or fine-tune any machine-learning or artificial-intelligence model unless Customer expressly authorizes such use in an applicable Order, through a setting controlled by an Administrator designated by Customer, or in another written authorization accepted by Redesign. Redesign and its Affiliates may use aggregated, de-identified, or anonymized data that does not identify Customer or any individual, and usage data, telemetry, performance data, diagnostic data, and interaction data that do not include Customer workload content, to develop, train, fine-tune, test, evaluate, validate, operate, and improve Redesign's models, systems, products, and services. If Customer authorizes training on identifiable Customer Data, Redesign and its Affiliates may retain and use resulting models, model parameters, weights, embeddings, statistical information, and improvements after expiration, termination, or prospective revocation of the authorization, provided such materials do not identify Customer or any individual and are not designed to reproduce Customer Data. Customer may revoke an Administrator-controlled training authorization prospectively through the applicable setting. Revocation does not require Redesign or its Affiliates to retrain, reverse, or remove improvements made before revocation became effective.

7. Connectors, Integrations, APIs, and Third-Party Services

7.1 Customer Authorization. Customer authorizes Redesign to use Connectors approved, configured, enabled, or provided by Customer to access Customer Systems, Third-Party Services, data sources, applications, models, tools, and environments as necessary to provide the Redesign Products and Redesign Applications.

7.2 Connector Configuration. Customer is responsible for approving Connector scope, permissions, credentials, rate limits, data sources, environments, and access levels. Redesign may rely on Customer's approvals, instructions, credentials, and configurations.

7.3 Connector Dependencies. Connectors may depend on third-party APIs, authentication, credentials, permissions, rate limits, schemas, network connectivity, and source-system availability. Redesign is not responsible for failures or delays caused by those dependencies unless expressly stated otherwise in the applicable Order.

7.4 Third-Party Services. Third-Party Services are subject to the applicable third-party terms. Redesign is not responsible for Third-Party Services, including their availability, security, performance, output, acts, omissions, data handling, models, support, service levels, changes, suspension, or termination.

7.5 Customer Credentials. Customer is responsible for ensuring that all credentials, tokens, keys, and service accounts made available to Redesign or configured in a Redesign Product have the required permissions and comply with applicable third-party terms and Customer policies.

redesign

7.6 API and Rate Limits. Customer will not use any API, Connector, Redesign Product, Redesign Application, or related functionality in a manner that exceeds applicable rate limits, usage limits, entitlement limits, technical restrictions, Documentation, third-party limits, or Order limits.

7.7 Changes to Third-Party Services. Redesign is not responsible for failures, delays, reduced functionality, security issues, data loss, stale data, or performance issues caused by changes to Third-Party Services, APIs, permissions, models, terms, pricing, access requirements, or technical restrictions.

8. Audit Logs, Administrative Logs, and System Records

8.1 Logs. Redesign may create and maintain logs, records, metadata, and system events relating to login activity, session activity, permission changes, Administrator actions, entitlement changes, Connector activity, workflow execution, API calls, support activity, security events, configuration changes, and other activity within or relating to Redesign Products or Redesign Applications.

8.2 Use of Logs. Redesign may use logs and system records to provide, secure, troubleshoot, support, maintain, improve, and administer the Redesign Products and Redesign Applications; investigate issues; verify usage; enforce entitlements; detect abuse; and comply with applicable Law.

8.3 Customer Access to Logs. Customer access to logs, exports, audit trails, or administrative records will be provided only to the extent included in the applicable Order, available functionality, Documentation, or Redesign's then-current standard practices.

8.4 Retention. Redesign may retain logs and system records in accordance with its standard retention practices, subject to the DPA where logs contain Personal Data.

9. Restrictions

Customer will not, and will not permit any Authorized User or third party to:

- (a) copy, modify, translate, adapt, or create derivative works of the Redesign Products, Redesign Applications, Documentation, Provider Technology, Redesign Configurations, or Redesign intellectual property except as expressly permitted in the Documentation;
- (b) reverse engineer, decompile, disassemble, or otherwise attempt to derive source code, object structure, architecture, non-public APIs, models, algorithms, workflows, or underlying proprietary information;
- (c) sell, resell, license, sublicense, distribute, rent, lease, timeshare, outsource, host, or make Redesign Products or Redesign Applications available to any third party;
- (d) use Redesign Products or Redesign Applications to provide services to third parties unless expressly authorized in an applicable Order;
- (e) bypass, disable, interfere with, or circumvent entitlement controls, security controls, license keys, rate limits, usage limits, access controls, telemetry, purchasing controls, or technical restrictions;
- (f) introduce malicious code, interfere with the security or operation of Redesign Products or Redesign Applications, or attempt unauthorized access to Redesign systems or other customers' data;
- (g) use Redesign Products, Redesign Applications, or Output to build, benchmark, train, evaluate, or improve a competing product or service;
- (h) publish or disclose benchmark, availability, security, or performance results without Redesign's prior written consent;
- (i) use Redesign Products or Redesign Applications with unsupported, unlicensed, unauthorized, or end-of-life systems except as expressly approved by Redesign in writing;
- (j) use Redesign Products or Redesign Applications for High-Risk Use, including systems where failure could reasonably result in death, serious bodily injury, severe physical damage, or severe environmental damage;
- (k) use Redesign Products or Redesign Applications in violation of applicable Law, third-party rights, third-party terms, Documentation, the Agreement, or applicable Orders; or
- (l) conduct or attempt any penetration testing, vulnerability scanning, red-teaming, load or stress testing, adversarial testing, prompt-injection testing, or other security or intrusion testing of Redesign Products, Redesign Applications, or Redesign infrastructure without Redesign's prior written authorization specifying the scope, timing, method, and environment of such testing; provided that this restriction does not limit testing confined entirely to Customer's own on-premises or customer-hosted instance in an environment that Redesign does not host, operate, or control, as described in Section 3.2.



10. Security

10.1 Redesign Security. Redesign will maintain administrative, technical, and physical safeguards designed to protect Personal Data in Redesign's possession, custody, or control in accordance with the DPA.

10.2 Customer Security. Customer is responsible for maintaining security in Customer Systems, including network security, identity systems, MFA, privileged access, endpoint protection, logging, monitoring, patching, vulnerability management, backups, business continuity, physical security, user training, purchasing controls, and Administrator controls.

10.3 Shared Responsibility. Security for Redesign Products and Redesign Applications depends on both parties' performance of their respective responsibilities. Redesign is not responsible for Security Breaches, incidents, outages, data loss, unauthorized access, unauthorized purchases, unauthorized approvals, or performance issues caused by Customer Systems, Customer Data, Customer credentials, Customer instructions, Third-Party Services, Customer's failure to follow Documentation, Customer's failure to maintain security controls, or actions by Customer or Authorized Users.

10.4 Security Actions. Redesign may suspend access, disable functionality, rotate credentials, revoke tokens, throttle activity, require configuration changes, or take other reasonable actions if Redesign determines that continued access or activity may create a security, legal, operational, availability, data integrity, procurement, supplier, or third-party risk.

10.5 Authorized Security Testing. Redesign may permit scoped security testing of Redesign Products, Redesign Applications, or Redesign infrastructure under a separate written authorization. Any authorized testing must: (a) be conducted against non-production or staging environments where required by Redesign; (b) follow the scope, timing, method, and environment specified in the authorization; (c) not access, target, or attempt to access other customers' data, tenants, or environments; (d) not degrade, disrupt, or attempt to degrade shared infrastructure or other customers' use; and (e) require that all findings be reported to Redesign in accordance with Section 10.6 before any third-party or public disclosure. Redesign may suspend or revoke testing authorization at any time if testing creates a security, availability, legal, or third-party risk.

10.6 Responsible Disclosure. If Customer or any Authorized User discovers or becomes aware of any vulnerability, security flaw, misconfiguration, or exploit in any Redesign Product, Redesign Application, or Redesign infrastructure, whether through authorized testing under Section 10.5 or in the normal course of use, Customer will: (a) promptly report it to Redesign in writing; (b) treat the existence and details of the vulnerability as Redesign's Confidential Information; (c) not exploit or leverage the vulnerability beyond the minimum necessary to identify and report it, and not use it to access, alter, or exfiltrate any data, including other customers' data; and (d) not disclose the vulnerability to any third party or publicly until Redesign has had a reasonable period to investigate and remediate and has authorized disclosure. This Section applies regardless of whether any testing occurred.

11. Support, Maintenance, and Availability

11.1 Support Scope. Redesign will provide support for Redesign Products and Redesign Applications only to the extent expressly included in the applicable Order, Addendum, or Documentation.

11.2 Maintenance. Redesign may perform scheduled, emergency, and security maintenance for Redesign Products and Redesign Applications. Portions of the Redesign Products or Redesign Applications may be unavailable during maintenance.

11.3 Updates. Redesign may update, modify, patch, improve, deprecate, or discontinue features, APIs, Connectors, models, workflows, or components from time to time.

11.4 No General Availability Commitment. Unless expressly stated in an applicable Order, Redesign does not provide uptime, availability, response time, resolution time, service level, service credit, procurement timing, ordering availability, catalog availability, or performance commitments for the Redesign Products or Redesign Applications.

12. Suspension

12.1 Suspension Rights. Redesign may suspend Customer's or any Authorized User's access to any Redesign Product or Redesign Application if Customer: (a) fails to pay undisputed amounts when due; (b) exceeds entitlements, usage limits, or license scope; (c) violates the Agreement; (d) creates a security, legal, operational, procurement, supplier, or third-party risk; (e) violates applicable Law; (f) fails to maintain required prerequisites; (g) uses a Redesign Product or Redesign Application in a manner that could harm Redesign, Customer, other customers, suppliers, or third parties; or (h) materially interferes with the operation, security, or availability of Redesign Products or Redesign Applications.

redesign

12.2 Effect of Suspension. Suspension does not relieve Customer of payment obligations. Redesign is not liable for losses, damages, data unavailability, workflow interruption, procurement interruption, order delay, operational impact, or other consequences arising from a suspension permitted under the Agreement.

13. Warranties and Disclaimers

13.1 Limited Warranty. To the extent the Services Terms apply, Redesign's services warranty in the Services Terms applies to professional services expressly provided by Redesign under an applicable Order. To the extent an Addendum contains a product-specific warranty, that warranty applies only to the applicable Redesign Product or Redesign Application and only as stated in the Addendum.

13.2 General Disclaimer. Except as expressly stated in the Agreement or applicable Addendum, the Redesign Products, Redesign Applications, Output, Connectors, Documentation, APIs, workflows, reports, dashboards, agents, tools, and related functionality are provided "AS IS" and "AS AVAILABLE" without warranties of any kind.

13.3 No Specific Outcome. Redesign does not warrant that Redesign Products, Redesign Applications, Output, reports, workflows, agents, tools, Connectors, or integrations will be uninterrupted, error-free, vulnerability-free, fully secure, latency-free, performance-neutral, complete, accurate, current, non-infringing, suitable for any specific regulatory requirement, or sufficient for Customer's legal, compliance, audit, procurement, tax, accounting, operational, security, or business requirements.

13.4 Third-Party Disclaimer. Redesign makes no warranties with respect to Third-Party Services except to the extent an express warranty is passed through from the applicable third-party provider.

13.5 No Unauthorized Warranty. No representative of Redesign or its Affiliates is authorized to make any representation, warranty, commitment, indemnity, guarantee, procurement commitment, lifecycle commitment, or other obligation not expressly stated in the Agreement.

14. Indemnity and Liability

14.1 Redesign IP Indemnity. Subject to the exclusions, procedures, remedies, and limitations of liability in the Agreement and these Technology Terms, Redesign shall defend Customer against any third-party claim alleging that a Redesign Product or Redesign Application, as provided by Redesign and used by Customer in accordance with the Agreement, these Technology Terms, the applicable Addendum, the applicable Order, and the Documentation, infringes a United States patent, copyright, or trade secret, and shall pay damages finally awarded against Customer or amounts approved by Redesign in settlement.

14.2 IP Indemnity Exclusions. Redesign has no obligation under Section 14.1 for any claim arising from or relating to: (a) Customer Data; (b) Customer Systems; (c) Customer specifications, instructions, configurations, prompts, workflows, procurement instructions, or requirements; (d) Third-Party Services, Third-Party Models, open source software, third-party materials, or supplier data; (e) use with software, hardware, systems, models, data, or services not provided by Redesign; (f) modifications not made by Redesign; (g) use after Redesign provides a non-infringing workaround, update, replacement, or instruction to stop use; (h) use outside the licensed scope, applicable Order, Documentation, or entitlements; (i) Customer's breach of the Agreement, these Technology Terms, or any Addendum; or (j) Output.

14.3 IP Mitigation. If a Redesign Product or Redesign Application becomes, or Redesign reasonably believes may become, subject to an infringement claim, Redesign may, at its option: (a) procure the right for Customer to continue using the affected functionality; (b) modify the affected functionality so it is non-infringing; (c) replace the affected functionality with substantially similar non-infringing functionality; or (d) terminate the affected subscription or Order and refund prepaid unused fees for the affected functionality. This Section 14 states Customer's sole and exclusive remedy, and Redesign's entire liability, for infringement, misappropriation, or similar intellectual property claims.

14.4 IP Indemnity Procedure. Redesign's obligations under Section 14.1 are conditioned on Customer: (a) promptly notifying Redesign in writing of the claim; (b) giving Redesign sole control of the defense and settlement of the claim; (c) not making any admission, settlement offer, or prejudicial statement without Redesign's prior written consent; and (d) providing reasonable cooperation at Redesign's expense. Redesign will not settle any claim in a manner that admits fault by Customer or imposes non-monetary obligations on Customer without Customer's prior written consent, not to be unreasonably withheld.

14.5 Customer Indemnity. In addition to Customer's indemnification obligations under the Agreement, Customer will defend, indemnify, and hold harmless Redesign, its Affiliates, and its and their directors, officers, employees, agents, subcontractors, and licensors from and against all third-party Claims and Losses arising from or relating to: (a) Customer Data; (b) Customer Systems; (c)

redesign

Customer's or Authorized Users' use of the Redesign Products, Redesign Applications, Output, Connectors, agents, tools, or workflows; (d) Customer's breach of these Technology Terms or any Addendum; (e) Customer's violation of applicable Law or third-party rights; (f) Customer's failure to obtain required rights, consents, notices, permissions, or legal bases; (g) Customer's use of Output without appropriate review; (h) Customer's use of Third-Party Services; (i) Customer's failure to maintain required security controls, backups, procurement controls, approval controls, or prerequisites; or (j) orders, purchase approvals, procurement instructions, or purchasing activity submitted through Customer's account or procurement workflows.

14.6 Security Breach and Personal Data. Any Security Breach, privacy incident, Personal Data breach, unauthorized access to Personal Data, or other claim arising from Redesign's processing of Personal Data on behalf of Customer is governed by the DPA. Security incidents or unauthorized access involving Customer Data that is not Personal Data are governed by these Technology Terms, including Section 14.7. These Technology Terms do not create any additional Security Breach, privacy, data protection, or Personal Data processing obligations beyond those stated in the DPA.

14.7 Liability Cap. To the maximum extent permitted by applicable Law, and except for matters governed by the DPA under Section 14.6, Redesign's aggregate liability arising out of or relating to any Redesign Product, Redesign Application, any Addendum, Customer Data, Output, Third-Party Services, Connector, API, workflow, support, professional services, managed services, or any related services provided in connection with a Redesign Product or Redesign Application will not exceed \$10,000 in the aggregate. Notwithstanding the foregoing, Redesign's aggregate liability for its IP indemnification obligations under Section 14.1 shall not exceed the greater of one hundred thousand dollars (\$100,000) or the total fees paid by Customer under the applicable Order during the twelve (12) months preceding the event giving rise to the claim.

14.8 Exclusion of Damages. To the maximum extent permitted by applicable Law, Redesign will not be liable for loss of profits, loss of revenue, loss of business, loss of goodwill, loss or corruption of data, loss of use, system downtime, business interruption, replacement services, cover, incidental damages, consequential damages, indirect damages, special damages, exemplary damages, punitive damages, procurement delay, purchasing error, supplier delay, asset management error, lifecycle planning error, or damages arising from Customer Systems, Third-Party Services, Customer Data, Output, or Customer's use of Redesign Products or Redesign Applications.

14.9 Relationship to Addendums. This Section 14 applies to all Addendums, Redesign Products, and Redesign Applications unless an applicable Order expressly identifies the specific provision being modified and states that the modification is intended to amend this Section 14.

15. Order of Precedence

If Customer and Redesign have signed a separate written master agreement governing the applicable Redesign Product or Redesign Application, that master agreement controls over these Technology Terms unless the master agreement expressly provides otherwise. Subject to the foregoing, in the event of conflict among the documents governing Redesign Products or Redesign Applications, the following order of precedence applies:

- (a) the applicable Order, but only to the extent it expressly identifies the provision being modified and states that it is intended to modify that provision;
- (b) the DPA, solely with respect to the processing of Personal Data;
- (c) the applicable Addendum, solely with respect to the applicable Redesign Product or Redesign Application;
- (d) the Product Sales Terms and Conditions, solely with respect to purchases of hardware, software, subscriptions, support, maintenance, service entitlements, Redesign Products, Redesign Applications, and related product purchases;
- (e) the Third-Party Services Terms and Conditions, solely with respect to Third-Party Services;
- (f) the Services Terms and Conditions, solely with respect to Redesign services provided in connection with Redesign Products or Redesign Applications;
- (g) these Technology Terms; and
- (h) Documentation, solely for technical, administrative, and usage instructions.

16. Termination and Effect of Termination

16.1 Term. These Technology Terms apply for so long as Customer accesses or uses any Redesign Product or Redesign Application.

redesign

16.2 Termination. Termination rights are governed by the Agreement and applicable Orders. Redesign may terminate or disable access to any Redesign Product or Redesign Application as permitted under the Agreement, applicable Addendum, or these Technology Terms.

16.3 Effect of Termination. Upon expiration or termination of the applicable Order or access right: (a) Customer's right to access and use the affected Redesign Products and Redesign Applications will terminate; (b) Customer will cease all use of the affected functionality; (c) Redesign may disable accounts, entitlements, Connectors, workflows, agents, and access; and (d) Customer will pay all amounts due or that become due under the Agreement.

16.4 Data Export and Deletion. Data export, return, deletion, and retention are governed by the DPA, applicable Addendum, applicable Order, available export functionality, and Redesign's standard retention practices.

16.5 Survival. Sections 1, 5, 6, 7.3 through 7.7, 8, 9, 10, 13, 14, 15, 16.3 through 16.5, and 17 survive expiration or termination.

17. General

17.1 Modifications. Redesign may modify these Technology Terms from time to time by posting an updated version at Redesign's legal terms page. Unless an Order expressly incorporates a prior version by version date, the version posted at the time Redesign accepts the applicable Order will govern that Order. For ongoing subscriptions and services, updated Technology Terms will apply prospectively beginning on the earliest date permitted under the applicable Agreement.

17.2 Governing Law and Dispute Resolution. Governing law, venue, arbitration, claim limitations, notices, assignment, publicity, force majeure, confidentiality, anti-corruption, compliance with laws, and other general provisions are governed by the Agreement.

Addendum A: Unified Portal, Marketplace, and Asset Management

This Addendum supplements the Technology Terms and governs Customer's access to and use of the Unified Portal, Marketplace Functionality, and Asset Management Functionality. This Addendum applies only if the Unified Portal, Marketplace Functionality, or Asset Management Functionality is included in an Order, enabled for Customer, or otherwise made available by Redesign to Customer.

A1. Definitions

A1.1 "Asset Data" means data, records, metadata, attributes, classifications, identifiers, configuration information, telemetry, ownership information, location information, lifecycle information, entitlement information, warranty information, support information, end-of-life information, end-of-support information, security information, vulnerability information, usage information, procurement information, licensing information, and other information relating to Customer's hardware, software, cloud resources, virtual machines, endpoints, network devices, applications, subscriptions, users, identities, licenses, services, and other technology assets.

A1.2 "Asset Management Functionality" means asset inventory, asset management, discovery, enrichment, classification, normalization, lifecycle tracking, entitlement tracking, support-status tracking, warranty-status tracking, end-of-life tracking, refresh planning, reporting, dashboards, recommendations, and related functionality.

A1.3 "Asset Source" means any Customer System, Third-Party Service, API, Connector, agent, upload, scan, discovery tool, CMDB, EDR, MDM, IAM system, network management tool, cloud console, ticketing system, procurement system, licensing system, manufacturer portal, distributor portal, support database, warranty database, or other source from which Asset Data is collected, imported, discovered, synchronized, indexed, analyzed, or generated.

A1.4 "Lifecycle Recommendations" means recommendations, alerts, reports, dashboards, summaries, forecasts, or other Output generated or displayed relating to upgrades, replacements, renewals, end-of-life, end-of-support, refresh cycles, license optimization, support coverage, warranty status, compatibility, security posture, vulnerability exposure, lifecycle planning, procurement timing, and related asset management matters.

A1.5 "Lifecycle Services" means lifecycle management, procurement planning, renewal support, asset reconciliation, software asset management, license optimization, refresh planning, upgrade planning, replacement planning, warranty or support review, remediation planning, or related services provided by Redesign under an applicable Order or SOW.

A1.6 "Marketplace Functionality" means marketplace, catalog, quoting, ordering, renewal, procurement, checkout, approval-routing, asset refresh, replacement, upgrade, lifecycle, and related functionality.

A1.7 "Portal Asset" means a digital record, listing, entitlement, object, module, application, product record, subscription record, license record, service entitlement record, hardware record, software record, cloud resource record, endpoint record, network device record, virtual machine record, lifecycle item, procurement item, support item, warranty item, or other asset-related record displayed, tracked, managed, enabled, ordered, renewed, accessed, or administered through or in connection with the Unified Portal. For clarity, a Portal Asset record does not alter ownership of, title to, risk of loss for, or contractual rights in the underlying product, service, hardware, software, subscription, license, entitlement, or other asset.

A1.8 "Unified Portal" means Redesign's centralized access, identity, entitlement, administration, navigation, marketplace, asset management, and user interface layer through which Customer and its Authorized Users may access Redesign Products, Redesign Applications, Portal Assets, Marketplace Functionality, Asset Management Functionality, and related functionality enabled under an applicable Order.

A2. Unified Portal Access

A2.1 Portal Access. Subject to the Technology Terms and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use the Unified Portal and enabled functionality solely for Customer's internal business purposes.

A2.2 Switch Component. The Unified Portal may include functionality that allows Authorized Users to navigate between Redesign Products and Redesign Applications they are authorized to access without logging in again.

A2.3 Portal-Specific Administration. Unified Portal administrators may enable or disable Redesign Applications for each Customer organization, manage user access within applications, configure entitlements, and administer Portal Assets, Marketplace Functionality, and Asset Management Functionality.

A3. Asset Management, Lifecycle Recommendations, and Lifecycle Services

A3.1 Asset Management Functionality. The Unified Portal may include Asset Management Functionality for Portal Assets and other technology assets identified, displayed, managed, or tracked in the Unified Portal.

A3.2 Asset Sources. Customer authorizes Redesign to access, collect, import, discover, scan, synchronize, index, analyze, normalize, enrich, classify, display, store, and generate Output from Asset Data obtained from Asset Sources enabled, approved, or made available by Customer or Redesign.

A3.3 Lifecycle Recommendations. The Unified Portal may generate or display Lifecycle Recommendations. Lifecycle Recommendations are informational and operational planning tools only. They are based on available Asset Data, Customer Systems, Third-Party Services, manufacturer information, distributor information, support data, warranty data, usage data, configuration data, vulnerability data, licensing data, and Customer-approved settings. Customer is responsible for reviewing, validating, and approving Lifecycle Recommendations before relying on them or using them for procurement, budgeting, compliance, security, operational, legal, financial, accounting, tax, audit, customer-facing, or remediation purposes.

A3.4 No Procurement Commitment. A Lifecycle Recommendation does not constitute a quote, purchase commitment, statement of work, order, renewal notice, binding procurement recommendation, compatibility warranty, pricing guarantee, inventory guarantee, availability guarantee, or commitment by Redesign or any Third-Party Service provider to provide, support, replace, upgrade, renew, remediate, or continue any product, service, subscription, license, support entitlement, warranty, or Portal Asset.

A3.5 Lifecycle Services. Redesign may provide Lifecycle Services only if expressly included in an applicable Order or SOW. Lifecycle Services are governed by the Agreement, the Services Terms and Conditions, and the applicable Order or SOW.

A3.6 Customer Responsibility. Customer remains responsible for asset ownership, asset governance, lifecycle decisions, procurement decisions, budget approvals, security remediation, patching, replacement, upgrade, decommissioning, licensing, entitlement compliance, warranty decisions, support decisions, CMDB governance, regulatory compliance, accounting treatment, and all decisions based on Asset Data or Lifecycle Recommendations.

A3.7 Data Quality and Freshness. Asset Data and Lifecycle Recommendations may be incomplete, inaccurate, duplicative, inconsistent, misclassified, outdated, or affected by source-system limitations, synchronization frequency, rate limits, permissions, unsupported assets, offline devices, shadow IT, unmanaged systems, incomplete credentials, naming inconsistencies, manufacturer data, distributor data, third-party data errors, or Customer configuration. Redesign does not warrant that Asset Data or Lifecycle Recommendations will be complete, accurate, current, non-duplicative, or suitable for Customer's intended purpose.

A3.8 No System of Record. Unless expressly stated in an applicable Order or SOW, the Unified Portal is not Customer's system of record for accounting, tax, financial reporting, audit, procurement, compliance, legal, licensing, security, CMDB, or asset lifecycle purposes.

A3.9 No Compliance or Remediation Warranty. Redesign does not warrant that Asset Data, Lifecycle Recommendations, or Lifecycle Services will satisfy any law, regulation, audit, certification, customer requirement, insurer requirement, licensing requirement, software audit requirement, security framework, warranty requirement, support requirement, contractual requirement, or procurement requirement.

A3.10 No Remediation Obligation. Unless expressly stated in an applicable Order or SOW, Redesign has no obligation to remediate, patch, update, decommission, secure, classify, tag, correct, reconcile, procure, replace, upgrade, renew, or manage any Portal Asset or other asset identified in the Unified Portal.

A4. Marketplace Purchases

A4.1 Marketplace Functionality. The Unified Portal may include Marketplace Functionality through which Customer may request quotes, place orders, approve purchases, renew subscriptions, procure hardware, software, subscriptions, support, maintenance, service entitlements, Third-Party Services, Redesign Products, Redesign Applications, Portal Assets, and related offerings.

A4.2 Governing Terms. Marketplace purchases are governed by the Agreement, the applicable Order or quote, the Product Sales Terms and Conditions, the Third-Party Services Terms and Conditions, the Services Terms and Conditions, the DPA, and applicable third-party provider or supplier terms.

A4.3 Order Acceptance. Marketplace submission, cart creation, checkout, approval routing, purchase request, purchase order upload, quote request, or similar portal action does not obligate Redesign to accept, fulfill, procure, reserve, ship, deliver, renew, or provide any product or service. All Marketplace purchases are subject to Redesign's acceptance, third-party provider or supplier acceptance,

redesign

credit approval, availability, export review, fraud review, pricing confirmation, tax calculation, shipping confirmation, and applicable supplier or manufacturer requirements.

A4.4 Pricing and Availability. Marketplace pricing, availability, lead times, shipping dates, renewal dates, product descriptions, lifecycle information, warranty information, support status, compatibility information, and recommendations may be based on information from Redesign, distributors, manufacturers, third-party providers, catalogs, APIs, feeds, or other sources. Such information may be incomplete, inaccurate, delayed, stale, or subject to change without notice. Unless Redesign expressly accepts an Order with firm pricing, Redesign does not guarantee marketplace pricing, availability, lead times, discounts, rebates, promotions, product descriptions, lifecycle status, or compatibility.

A4.5 Third-Party Products and Supplier Terms. Hardware, software, subscriptions, support, maintenance, cloud services, service entitlements, and other third-party offerings available through Marketplace Functionality are provided by the applicable third-party supplier or provider and are subject to applicable third-party terms. Redesign is not responsible for third-party product performance, availability, warranties, recalls, support, security, vulnerabilities, compatibility, defects, infringement, product liability, shipping delays, end-of-life decisions, discontinuance, or supplier acts or omissions.

A4.6 Customer Responsibility for Orders. Customer is responsible for reviewing and validating all Marketplace orders, quantities, SKUs, part numbers, configurations, compatibility, shipping addresses, billing information, tax-exemption information, renewal terms, support terms, license quantities, subscription terms, user counts, device counts, entitlement terms, and Customer approvals before submission. Redesign may rely on Marketplace orders, approvals, purchase requests, and instructions submitted through Customer's account, Authorized Users, Administrators, procurement workflows, or connected systems.

A4.7 Hardware Purchases. Hardware purchased through Marketplace Functionality is subject to the Product Sales Terms and Conditions.

A4.8 Non-Cancellable Commitments. Orders for Third-Party Services, software, SaaS, cloud services, subscriptions, support, maintenance, service entitlements, custom configurations, special-order hardware, build-to-order hardware, and other non-standard, supplier-committed, or third-party-committed items may be non-cancellable and non-refundable once submitted to Redesign, a distributor, manufacturer, supplier, or third-party provider.

A4.9 Approvals and Authority. Customer is responsible for configuring and maintaining all Marketplace approval workflows, purchasing permissions, Administrators, approvers, procurement rules, spending limits, budget controls, cost centers, ship-to locations, bill-to information, and user access. Redesign may treat any order, approval, purchase request, or instruction submitted through Customer's Marketplace account or procurement workflow as authorized by Customer.

A4.10 Errors and Corrections. Redesign may reject, cancel, correct, or modify Marketplace quotes, orders, pricing, tax, shipping, product information, availability, or other information affected by errors, omissions, supplier changes, catalog errors, typographical errors, system errors, expired pricing, fraud concerns, export restrictions, or other issues before Redesign accepts the applicable Order.

A4.11 No Marketplace Warranty. Redesign does not warrant that Marketplace Functionality, catalogs, product listings, lifecycle recommendations, compatibility information, pricing, availability, approval workflows, procurement integrations, or ordering features will be uninterrupted, error-free, current, complete, accurate, compatible with Customer's procurement systems, or suitable for Customer's purchasing, compliance, tax, accounting, budgeting, audit, or operational requirements.

A4.12 Purchase Data. Customer authorizes Redesign to process Marketplace order data, procurement data, approval data, Asset Data, billing data, shipping data, renewal data, entitlement data, usage data, and related information as necessary to provide Marketplace Functionality, administer orders, support renewals, maintain asset records, generate Lifecycle Recommendations, support billing, comply with Law, and enforce the Agreement. The DPA applies only to the extent Redesign processes Personal Data on behalf of Customer.



Addendum B: OpenCloud

This OpenCloud Addendum supplements the Technology Terms and governs Customer's access to and use of OpenCloud. This Addendum applies only if OpenCloud is included in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer.

B1. Definitions

B1.1 "API" means any application programming interface made available by Redesign for OpenCloud.

B1.2 "Customer Environment" means the servers, storage, networks, systems, facilities, software, data center, cloud, colocation, or other technology environment owned, leased, operated, or controlled by Customer or its authorized Affiliates where OpenCloud or the Supported Stack is installed, hosted, accessed, or managed.

B1.3 "Node" means each physical server, host, compute node, or other infrastructure node in the Customer Environment that is managed by, connected to, provisioned through, or otherwise enabled for use with OpenCloud, OpenStack, KVM, Kubernetes, or any other component of the Supported Stack. Unless the applicable Order states otherwise, all Nodes in a cluster or environment managed by OpenCloud must be licensed and under vendor support.

B1.4 "Open Source Components" means third-party open source software, community edition software, and related components used with or underlying the OpenCloud deployment, including but not limited to: OpenStack, KVM, Kubernetes, ArgoCD, Prometheus, Loki, Grafana, Headlamp, and related dependencies.

B1.5 "OpenCloud" means Redesign's proprietary private cloud provisioning, management, and orchestration software, including updates, connectors, APIs, user interfaces, scripts, templates, workflows, and Documentation made available by Redesign under an applicable Order.

B1.6 "Preview Feature" means any beta, preview, pre-release, evaluation, experimental, or similar feature, functionality, integration, API, or capability made available by Redesign for testing, evaluation, or early access.

B1.7 "Supported Stack" means OpenCloud and the Open Source Components, third-party software, configurations, storage integrations, observability tools, and related components expressly identified as supported in the applicable Order.

B2. OpenCloud Subscription License

B2.1 License Grant. Subject to Customer's payment of all applicable fees and compliance with the Agreement, the Technology Terms, this Addendum, and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable subscription license during the applicable subscription term to install, access, and use OpenCloud solely in the Customer Environment, solely for Customer's and its authorized Affiliates' internal business purposes, and solely up to the number of licensed Nodes identified in the applicable Order.

B2.2 No Perpetual Rights. OpenCloud is licensed on a subscription basis only. Customer receives no perpetual license, ownership interest, or continuing right to use OpenCloud after expiration or termination of the applicable subscription term.

B2.3 Node-Based Entitlement. Customer must maintain an active subscription for each Node managed by, connected to, provisioned through, or otherwise enabled for use with OpenCloud. If Customer adds Nodes during a subscription term, Redesign may invoice Customer for the additional Nodes at the rates stated in the applicable Order or, if no rate is stated, at Redesign's then-current rates.

B2.4 Minimum Commitment. Unless otherwise stated in the applicable Order, Customer may not reduce the number of licensed Nodes during the initial subscription term below the number of Nodes identified in the first invoice or Order.

B2.5 Non-Cancellable Commitment. Unless expressly stated otherwise in the applicable Order, OpenCloud subscriptions are non-cancellable during the subscription term, and all fees for the full subscription term are non-refundable and remain payable.

Termination, suspension, non-use, reduction in Nodes, decommissioning of workloads, or Customer's transition to another platform does not relieve Customer of its obligation to pay all fees due for the full subscription term.

B3. Open Source Components

B3.1 Separate Licensing. Open Source Components are licensed under their respective open source licenses and are not licensed under this Addendum. Nothing in this Addendum limits Customer's rights under applicable open source licenses.

B3.2 No Sale of Open Source Components. Fees for OpenCloud are for Redesign's proprietary software, Documentation, deployment rights, maintenance, support, and related services. Redesign does not sell Open Source Components as proprietary software.

redesign

B3.3 Customer Compliance. Customer is responsible for complying with open source licenses applicable to Customer's use, modification, distribution, or operation of Open Source Components, except to the extent Redesign expressly assumes a specific obligation in the applicable Order.

B3.4 No Open Source Warranty. Redesign does not warrant Open Source Components except to the extent expressly stated in the applicable Order. Open Source Components are provided subject to their applicable licenses, community support models, and upstream release practices.

B3.5 Upstream Changes. Redesign is not responsible for delays, vulnerabilities, incompatibilities, feature changes, removals, end-of-life events, or other issues arising from upstream open source projects, except to the extent caused by Redesign's gross negligence or willful misconduct.

B4. Customer Environment and Shared Responsibilities

B4.1 Customer Infrastructure Responsibilities. Customer is responsible for providing and maintaining all hardware, storage, network connectivity, internet access, power, cooling, rack space, physical security, system access, facilities, vendor maintenance, and environmental conditions required for OpenCloud and the Supported Stack.

B4.2 Customer Operational Responsibilities. Customer is responsible for workloads, virtual machines, applications, operating systems, containers, images, tenant configurations, data, customer-side network configurations, firewall rules, identity integrations, access controls, tenant permissions, user administration, backups, disaster recovery, business continuity, required licenses, required consents, Customer Environment security controls, and compliance with laws and regulatory requirements applicable to Customer's use of OpenCloud.

B4.3 Redesign Responsibilities. Redesign is responsible only for providing the OpenCloud software license described in this Addendum, performing deployment, implementation, support, or managed services expressly stated in the applicable Order or SOW, maintaining safeguards for Personal Data in Redesign's possession, custody, or control as required by the DPA, and using commercially reasonable efforts to provide updates, patches, workarounds, or support as expressly stated in the applicable Order.

B4.4 Prerequisites. Customer must satisfy the prerequisites, assumptions, and minimum technical requirements stated in the applicable Order, Documentation, and Redesign's minimum security requirements.

B4.5 Customer Changes. Customer shall not make material changes to the OpenCloud environment, Supported Stack, network, storage, identity systems, security controls, or managed Nodes without providing Redesign prior notice and a reasonable opportunity to review the change. Redesign is not responsible for failures, outages, degradation, or security incidents caused by unauthorized or uncoordinated changes.

B5. Support and Managed Services

B5.1 Separate Support Scope. OpenCloud support, managed services, lifecycle management, patching, monitoring, incident response, and operational support are provided only if expressly included in the applicable Order or a separate managed services SOW.

B5.2 Covered Stack. Support applies only to the Supported Stack and licensed Nodes identified in the applicable Order. Support does not apply to unsupported hardware, unsupported software, customer-modified code, custom integrations, unlicensed Nodes, third-party services outside Redesign's control, or components excluded in the applicable Order.

B5.3 No Support for Unlicensed Nodes. Redesign has no obligation to support Nodes that are not licensed under an active OpenCloud subscription.

B5.4 Maintenance Windows. Redesign may perform scheduled, emergency, and security maintenance as provided in the applicable Order or managed services SOW. Customer acknowledges that OpenCloud, the Supported Stack, or portions of the Customer Environment may be unavailable during maintenance.

B5.5 Security Updates. Redesign may deploy or require Customer to deploy security patches, updates, configuration changes, or mitigations that Redesign reasonably determines are necessary to protect OpenCloud, the Supported Stack, Customer Environment, Redesign systems, or other customers.

B6. Usage Verification and Audit

B6.1 Usage Reporting. Upon Redesign's reasonable request, Customer shall provide Node counts, environment details, logs, configuration data, or other information reasonably necessary to verify usage, license compliance, and support eligibility.

redesign

B6.2 Technical Controls. Redesign may include license keys, entitlement controls, usage logs, telemetry, or other technical measures designed to validate licensed usage, provided that Redesign configures such measures in a manner designed to avoid collecting Customer workload content unless expressly required for support or security.

B6.3 Audit. Redesign may audit Customer's use of OpenCloud no more than once per twelve-month period unless Redesign reasonably believes Customer is materially out of compliance. Audits will be conducted during normal business hours, with reasonable advance notice, and in a manner designed to minimize disruption.

B6.4 True-Up. If an audit or usage report shows excess use, Customer shall promptly pay fees for all unlicensed Nodes from the date such Nodes were first used or, if that date cannot be determined, from the start of the then-current subscription term.

B7. Data, Warranties, and Termination

B7.1 Data Access and Portability. If OpenCloud stores Customer Data, configuration data, logs, environment metadata, or other Customer-controlled materials in systems controlled by Redesign, Redesign will make such materials available for export during the applicable subscription term using available export functionality or commercially reasonable export methods, subject to technical limitations and Customer's payment of applicable fees. Customer is responsible for exporting such materials before termination or expiration.

B7.2 No Sensitive Data by Default. Customer shall not provide Redesign access to Sensitive Data through OpenCloud unless the applicable Order expressly identifies the categories of Sensitive Data and any additional safeguards required.

B7.3 Warranty. During the subscription term, Redesign warrants that OpenCloud will materially conform to the Documentation when used in accordance with the Agreement, the Technology Terms, this Addendum, the applicable Order, and the Documentation. Customer's sole remedy for breach of this warranty is for Redesign, at its option, to use commercially reasonable efforts to correct the nonconformity or provide a workaround. If Redesign determines that correction or workaround is not commercially reasonable, Redesign may terminate the affected OpenCloud subscription and refund prepaid unused subscription fees for the affected OpenCloud license.

B7.4 Disclaimer. Except as expressly stated in this Addendum, OpenCloud, Open Source Components, Documentation, support, and related services are provided without warranties of any kind. Redesign does not warrant that OpenCloud or the Supported Stack will be uninterrupted, error-free, vulnerability-free, fully secure, compatible with all Customer workloads, or suitable for any specific regulatory, operational, or performance requirement.

B7.5 Effect of Expiration or Termination. Upon expiration or termination of the applicable subscription term, Customer shall cease using OpenCloud, uninstall or disable OpenCloud if requested by Redesign, and certify deletion or discontinuation upon request. Termination does not relieve Customer of payment obligations accrued before termination or payment obligations for the full subscription term.

B7.6 Operational Consequences. Customer acknowledges that expiration, termination, or suspension of OpenCloud may disable or degrade centralized management, provisioning, APIs, user interfaces, updates, automation, and support. Customer remains responsible for its workloads, data, underlying infrastructure, and any direct host-level or component-level management required after OpenCloud is disabled.



Addendum C: Redesign Exchange

This Redesign Exchange Addendum supplements the Technology Terms and governs Customer's access to and use of Redesign Exchange ("REX"). This Addendum applies only if REX is included in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer.

C1. Definitions

C1.1 "REX" means Redesign's file system discovery, indexing, analysis, data transfer, connection, and related unstructured data intelligence application.

C1.2 "REX Connector" means any Connector used with REX to access, scan, index, analyze, transfer, or connect to Customer Systems, file systems, repositories, applications, databases, storage environments, or Third-Party Services.

C1.3 "Source System" means any Customer System or Third-Party Service from which REX accesses, discovers, indexes, scans, analyzes, copies, exports, imports, transfers, or processes Customer Data.

C2. REX Access and Use

C2.1 Access Right. Subject to Customer's payment of all applicable fees and compliance with the Agreement, the Technology Terms, this Addendum, and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use REX solely for Customer's internal business purposes.

C2.2 REX Functionality. REX may provide file system discovery, indexing, analysis, classification, metadata extraction, data transfer, connector management, unstructured data intelligence, and connection to C7e Studio or other Redesign Applications, as described in the applicable Order or Documentation.

C2.3 Entitlements. Customer may use only the REX features, volumes, repositories, Source Systems, environments, Connectors, data sources, and transfer destinations authorized in the applicable Order or enabled by Redesign in writing.

C3. Customer Authorization and Responsibilities

C3.1 Access Authorization. Customer authorizes Redesign to use REX and REX Connectors to access, discover, scan, index, analyze, copy, transfer, and process Customer Data from Source Systems as configured or approved by Customer.

C3.2 Permissions. Customer is responsible for approving and maintaining REX Connector scope, permissions, credentials, service accounts, rate limits, repositories, file paths, source locations, destination locations, and access levels. Redesign may rely on Customer's approvals, instructions, credentials, and configurations.

C3.3 Least Privilege. Customer is responsible for configuring REX access on a least-privilege basis consistent with Customer's intended use, data governance requirements, and security policies.

C3.4 Source System Accuracy. Customer is responsible for identifying all Source Systems, data repositories, owners, custodians, permissions, restricted data categories, retention requirements, and legal or contractual restrictions relevant to REX.

C3.5 Sensitive Data. Customer shall not authorize REX to access Sensitive Data unless the applicable Order expressly identifies the relevant categories of Sensitive Data and required safeguards.

C4. Discovery, Indexing, Analysis, and Transfer

C4.1 Discovery and Indexing. Customer authorizes REX to discover, crawl, index, classify, tag, extract metadata from, and analyze Customer Data in authorized Source Systems. The index and associated metadata are stored in the location specified in the applicable Order. If the Order does not specify, the index is stored within the Customer's environment, and Redesign does not host or retain a copy unless access is required to provide support or related services under the applicable Order.

C4.2 Analysis and Extraction. Customer authorizes REX to analyze Customer Data, extract unstructured intelligence, identify patterns, generate summaries, create reports, and provide Output based on Customer Data.

C4.3 Data Transfer. Customer authorizes REX to copy, transfer, export, import, route, or synchronize Customer Data between approved Source Systems, destinations, Redesign Applications, and Third-Party Services as configured or approved by Customer.

C4.4 Validation. Customer is responsible for reviewing and validating transfer destinations, mappings, permissions, completeness, file integrity, data quality, and whether transferred data remains suitable for Customer's intended purpose.

redesign

C4.5 No Archival or Backup Obligation. Unless expressly stated in the applicable Order, REX is not a system of record, backup service, archival service, disaster recovery service, or legal hold system.

C5. Connector Operations, Data Freshness, and Pipeline Limitations

C5.1 Connector Dependencies. REX Connectors may depend on authentication flows, token refresh, credential validity, source-system availability, third-party APIs, pagination, rate limits, schema changes, retries, historical backfills, permissions, network connectivity, and data formats.

C5.2 Schema and Source Changes. Redesign is not responsible for failures, delays, stale data, duplicate data, missing data, incomplete syncs, interrupted transfers, or failed workflows caused by schema drift, API changes, field changes, permission changes, source-system changes, or third-party service changes.

C5.3 Retries and Failed Syncs. REX may attempt retries or error handling where supported by the applicable functionality. Redesign does not warrant that any failed sync, failed transfer, failed extraction, or failed workflow will be successfully retried, recovered, or completed.

C5.4 Historical Backfills. Historical backfills are provided only to the extent supported by the applicable Source System, Connector, entitlement, Order, and Documentation. Customer is responsible for validating the scope, completeness, and accuracy of backfilled data.

C5.5 Data Freshness. Indexed, ingested, transferred, extracted, or analyzed data may lag Source Systems and may become stale depending on sync frequency, Source System limits, rate limits, pipeline errors, permissions, data volume, network conditions, and Customer configuration. Redesign does not warrant real-time data freshness unless expressly stated in the applicable Order.

C6. Production System Performance

C6.1 Pipeline Design. Where Redesign designs or configures data ingestion pipelines for Customer's production systems, including ERP, MES, manufacturing, operational technology, or other critical systems, Redesign will use commercially reasonable efforts to design such pipelines to avoid material adverse impact on production system performance.

C6.2 Dependencies. Customer acknowledges that performance depends on Customer Systems, configurations, network conditions, Source System limitations, permissions, API limits, maintenance windows, data volumes, data formats, third-party limits, and Customer-approved access methods.

C6.3 No Absolute Performance Warranty. Unless expressly stated in an applicable Order, Redesign does not warrant uninterrupted, latency-free, or performance-neutral operation of Customer Systems.

C6.4 Customer Responsibilities. Customer is responsible for providing accurate system information, identifying critical systems, approving ingestion windows and rate limits, maintaining backups, validating test results, and promptly notifying Redesign of performance concerns.

C6.5 Protective Actions. Redesign may suspend, throttle, reschedule, or modify ingestion, indexing, scanning, transfer, or analysis activities if Redesign reasonably determines that continued activity may affect production system performance, security, availability, or data integrity.

C7. REX Disclaimers

C7.1 Source System Limitations. Redesign is not responsible for incomplete, delayed, inaccurate, corrupted, duplicated, or unavailable Customer Data caused by Source Systems, permissions, APIs, network conditions, third-party limits, file corruption, unsupported formats, or Customer configurations.

C7.2 Output. REX Output may be incomplete, inaccurate, stale, or dependent on available Customer Data, metadata, permissions, and Source System quality. Customer is responsible for validating REX Output before use.

C7.3 Third-Party Services. REX may connect to Third-Party Services. Redesign is not responsible for Third-Party Services or changes to their APIs, permissions, access controls, performance, availability, data formats, or terms.

redesign

Addendum D: Redesign C7e Enterprise AI Platform and AI Chat

This Addendum supplements the Technology Terms and governs Customer's access to and use of Redesign C7e Enterprise AI Platform, Redesign AI Chat, and related AI functionality. This Addendum applies only if Redesign C7e Enterprise AI Platform, AI Chat, or related AI functionality is included in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer.

D1. Definitions

D1.1 "AI Features" means artificial intelligence, machine learning, large language model, agentic, tool-calling, report-generation, workflow automation, and similar functionality made available by Redesign through the Redesign C7e Enterprise AI Platform or Redesign AI Chat.

D1.2 "AI Input" means prompts, files, documents, data, instructions, tools, context, model selections, workflow parameters, and other materials submitted to or made available for AI Features by or on behalf of Customer.

D1.3 "AI Output" means responses, reports, summaries, analyses, recommendations, classifications, extractions, workflow results, tool results, generated content, or other output generated by AI Features.

D1.4 "Redesign AI Chat" means Redesign's private artificial intelligence chat application, including functionality that may allow Customer to connect available models, connect tools, generate reports, and use agents or workflows.

D1.5 "Redesign C7e Enterprise AI Platform" means Redesign's artificial intelligence platform, applications, tools, agents, model access, workflows, and related services.

D1.6 "Third-Party Model" means any artificial intelligence model, large language model, embedding model, machine learning model, or similar technology not owned or controlled by Redesign.

D2. AI Access and Use

D2.1 Access Right. Subject to Customer's payment of all applicable fees and compliance with the Agreement, the Technology Terms, this Addendum, and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use Redesign C7e Enterprise AI Platform and Redesign AI Chat solely for Customer's internal business purposes.

D2.2 Enabled Features. Customer may use only the AI Features, models, tools, agents, workflows, usage volumes, and entitlements included in the applicable Order or enabled by Redesign in writing.

D2.3 Private AI Chat. Redesign AI Chat may allow Customer to submit prompts and files, connect available models, connect tools, generate reports, and use agents for workflow automation, subject to the applicable Order, Documentation, and Customer configurations.

D2.4 On-Premises Deployment. Where the Redesign C7e Enterprise AI Platform or Redesign AI Chat is deployed within Customer's own infrastructure using a private model that runs within Customer's environment, Customer Data, including AI Input and AI Output, may be processed entirely within Customer's environment and may not be transmitted to, accessed by, hosted by, or stored by Redesign. In such deployments: (a) Redesign's rights under Sections 6.2, 6.7, and D3.4 apply only to the extent Redesign actually receives or accesses such data in connection with support, troubleshooting, updates, training authorized by Customer, or other services expressly agreed in an applicable Order or SOW; (b) the DPA applies only to the extent Redesign processes Personal Data on behalf of Customer; and (c) Customer is solely responsible for the security, availability, performance, configuration, backups, data integrity, access controls, identity management, network security, and compliance of Customer's environment.

D3. AI Input, AI Output, and Ownership

D3.1 Customer Responsibility. Customer is responsible for AI Input and AI Output, including ensuring that AI Input and Customer's use of AI Output comply with applicable Law, third-party rights, the Agreement, the Technology Terms, this Addendum, and Customer's internal policies.

D3.2 Ownership of AI Input. As between Redesign and Customer, Customer retains all right, title, and interest in and to AI Input.

D3.3 Ownership of AI Output. As between Redesign and Customer, and to the extent permitted by applicable Law, Customer owns AI Output generated in response to Customer's AI Input, subject to Redesign's ownership of Redesign technology, Provider Technology, Redesign Configurations, models, tools, workflows, software, templates, know-how, and intellectual property, and subject to the licenses and rights granted to Redesign under Sections 6.2, 6.7, and D3.4.

redesign

D3.4 License to Redesign. Customer grants Redesign and its Affiliates a non-exclusive, worldwide, sublicensable, royalty-free license to use AI Input and AI Output as necessary to provide, secure, support, maintain, troubleshoot, and administer Redesign C7e Enterprise AI Platform and Redesign AI Chat; operate tools, models, and workflows; comply with applicable Law; and enforce the Agreement. Redesign may use identifiable AI Input and AI Output to develop, train, fine-tune, test, evaluate, validate, operate, or improve Redesign's machine-learning and artificial-intelligence models, systems, products, and services only as authorized under Section 6.7.

D3.5 Non-Uniqueness. AI Output may not be unique. Other customers or users may receive the same or similar output.

D4. Human Review and AI Disclaimers

D4.1 Output Disclaimer. AI Output may be incomplete, inaccurate, outdated, inappropriate, duplicative, non-unique, biased, or unsuitable for Customer's intended purpose. Redesign does not warrant that AI Output will be accurate, complete, current, reliable, non-infringing, or error-free.

D4.2 Human Review. Customer is responsible for implementing reasonable human review and validation before relying on, publishing, distributing, submitting, or using AI Output for legal, regulatory, compliance, financial, employment, safety, security, operational, or other material decisions.

D4.3 No Professional Advice. AI Output does not constitute legal, accounting, audit, tax, medical, financial, regulatory, cybersecurity, or other professional advice.

D4.4 Material Decisions. Customer shall not use AI Output as the sole basis for any decision that has legal or similarly significant effects, including decisions affecting employment, credit, lending, insurance, housing, healthcare, education, eligibility, legal rights, or access to material services.

D5. Third-Party Models and Customer Tools

D5.1 Third-Party Models. If Customer connects, selects, or uses a Third-Party Model, Customer's use of that model may be subject to third-party terms. Redesign is not responsible for Third-Party Models, including their availability, performance, security, data handling, training practices, output, infringement risk, or changes.

D5.2 Customer Tools. Customer is responsible for tools, APIs, systems, credentials, permissions, and data sources connected to Redesign C7e Enterprise AI Platform or Redesign AI Chat by or on behalf of Customer.

D5.3 Customer Actions. Customer is responsible for all decisions, actions, omissions, workflows, approvals, configurations, connected tool use, and external communications arising from or relating to Customer's use of AI Features or AI Output.

D6. AI Use Restrictions

Customer shall not use Redesign C7e Enterprise AI Platform, Redesign AI Chat, AI Features, or AI Output to:

- (a) violate applicable Law or third-party rights;
- (b) generate malware, phishing, scams, unlawful surveillance, or harmful code;
- (c) represent AI Output as human-generated when that representation would be inaccurate, misleading, or unlawful;
- (d) develop, train, or improve a product or service that competes with Redesign;
- (e) extract models, model weights, prompts, system instructions, or non-public model behavior;
- (f) circumvent safeguards, rate limits, safety controls, or usage restrictions;
- (g) submit health data, payment card data, classified information, export-controlled data, biometric data, children's data, or other restricted data unless expressly authorized in the applicable Order; or
- (h) make fully automated decisions with legal or similarly significant effects without appropriate human review and legal basis.

D7. AI-Specific Indemnity

In addition to Customer's indemnification obligations under the Agreement and Technology Terms, Customer will defend, indemnify, and hold harmless Redesign from third-party Claims and Losses arising from or relating to: (a) Customer's AI Input; (b) Customer's use of AI Output; (c) Customer's failure to apply human review; (d) Customer's connected tools, models, or data sources; (e) Customer's representation that AI Output was human-generated when it was not; or (f) Customer's use of Redesign C7e Enterprise AI Platform, Redesign AI Chat, or AI Features in violation of this Addendum.



Addendum E: Redesign GRC

This Redesign GRC Addendum supplements the Technology Terms and governs Customer's access to and use of Redesign GRC. This Addendum applies only if GRC is included in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer.

E1. Definitions

E1.1 "Compliance Materials" means reports, dashboards, control mappings, evidence summaries, readiness assessments, tasks, workflows, findings, risk ratings, recommendations, exports, and other materials generated by or through GRC.

E1.2 "Framework" means a security, privacy, governance, risk, compliance, audit, regulatory, certification, control, contractual, or policy framework configured in GRC.

E1.3 "GRC" means Redesign's governance, risk, and compliance application for evidence collection, control mapping, framework tracking, dashboards, reports, and compliance-related workflow automation.

E2. GRC Access and Use

E2.1 Access Right. Subject to Customer's payment of all applicable fees and compliance with the Agreement, the Technology Terms, this Addendum, and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use GRC solely for Customer's internal business purposes.

E2.2 GRC Functionality. GRC may provide automated and continuous compliance reporting, evidence collection, framework mapping, dashboards, reports, control tracking, task workflows, and related functionality, as described in the applicable Order or Documentation.

E2.3 Configured Frameworks. Customer may use only the Frameworks, integrations, reports, workflows, and features included in the applicable Order or enabled by Redesign in writing.

E3. Customer Responsibilities

E3.1 Framework Selection. Customer is responsible for determining which Frameworks, controls, evidence, policies, laws, regulations, contractual requirements, audit requirements, customer requirements, and certification requirements apply to Customer.

E3.2 Evidence Sources. Customer is responsible for selecting, connecting, approving, and maintaining evidence sources, data sources, integrations, credentials, permissions, personnel, control owners, and workflows.

E3.3 Accuracy of Customer Data. Compliance Materials depend on Customer Data, Customer Systems, Third-Party Services, configured sources, permissions, evidence quality, and Customer instructions. Customer is responsible for the accuracy, completeness, and currency of Customer Data and evidence.

E3.4 Review and Validation. Customer is responsible for reviewing, validating, approving, and determining the accuracy, completeness, and suitability of all Compliance Materials before relying on them or providing them to auditors, regulators, customers, insurers, certification bodies, or third parties.

E4. Regulatory Change and Framework Mapping

E4.1 Regulatory Change. GRC may include features intended to help Customer track, map, or manage regulatory, Framework, control, policy, or audit-related changes. Customer remains responsible for interpreting changes, determining applicability, updating controls, approving remediation, and deciding whether Customer's compliance program satisfies applicable requirements.

E4.2 Framework Mapping. Any control mapping, Framework mapping, requirement mapping, gap analysis, or recommendation generated by GRC is for workflow and informational purposes only. Customer is responsible for confirming that mappings are accurate, complete, current, and appropriate for Customer's industry, jurisdiction, customers, auditors, regulators, and contractual commitments.

E4.3 Regulatory Updates. Redesign does not warrant that GRC will identify every regulatory update, Framework update, control change, audit requirement, customer requirement, or compliance obligation applicable to Customer.

E5. No Audit, Certification, or Legal Advice

E5.1 No Certification. GRC does not certify, attest, verify, audit, or guarantee Customer's compliance with any Framework, law, regulation, contract, policy, control standard, or certification requirement.

redesign

E5.2 No Professional Advice. GRC does not provide legal, audit, accounting, tax, regulatory, cybersecurity, certification, or professional advice.

E5.3 Auditor and Regulator Decisions. Customer acknowledges that auditors, regulators, certification bodies, customers, insurers, and other third parties may reject, question, interpret, or require supplementation of Compliance Materials.

E6. GRC Disclaimers

E6.1 No Compliance Warranty. Redesign does not warrant that GRC or any Compliance Materials will satisfy any law, regulation, audit, certification, customer requirement, insurer requirement, Framework, or contractual requirement.

E6.2 No Reliance Without Review. Customer shall not rely on Compliance Materials without appropriate review, validation, and approval by qualified personnel.

E6.3 Third-Party Frameworks. Third-party Frameworks, standards, and control materials may be subject to third-party rights, terms, interpretations, and updates. Redesign is not responsible for third-party Framework changes or interpretations.



Addendum F: C7e Studio

This C7e Studio Addendum supplements the Technology Terms and governs Customer's access to and use of C7e Studio. This Addendum applies only if C7e Studio is included in an Order, deployed in Customer's environment, enabled in the Unified Portal, or otherwise made available by Redesign to Customer.

F1. Definitions

F1.1 "C7e Studio" or "Studio" means Redesign's application for unstructured intelligence extraction, data transformation, workflow design, analytics, automation, and related functionality.

F1.2 "Studio Output" means extracted, classified, transformed, structured, enriched, summarized, analyzed, or generated materials produced by or through Studio.

F1.3 "Workflow" means any workflow, pipeline, agent, process, automation, prompt chain, transformation, classification, routing, or extraction process configured or run through Studio.

F2. Studio Access and Use

F2.1 Access Right. Subject to Customer's payment of all applicable fees and compliance with the Agreement, the Technology Terms, this Addendum, and the applicable Order, Redesign grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable subscription term or Order term to access and use Studio solely for Customer's internal business purposes.

F2.2 Studio Functionality. Studio may provide unstructured intelligence extraction, data transformation, workflow design, analytics, automation, classification, summarization, and related functionality, as described in the applicable Order or Documentation.

F2.3 Entitlements. Customer may use only the Studio features, volumes, Workflows, data sources, destinations, and integrations authorized in the applicable Order or enabled by Redesign in writing.

F3. Customer Data and Studio Output

F3.1 Processing Authorization. Customer authorizes Redesign to use Studio to access, process, analyze, classify, extract, transform, structure, enrich, summarize, route, and generate Studio Output from Customer Data as necessary to provide Studio functionality.

F3.2 Customer Ownership. As between Redesign and Customer, Customer retains all right, title, and interest in Customer Data and, to the extent permitted by applicable Law, owns Studio Output generated from Customer Data.

F3.3 Redesign Ownership. Redesign and its licensors retain all right, title, and interest in Studio, Workflows, templates, connectors, methods, models, software, scripts, configurations, know-how, and Redesign intellectual property.

F3.4 Review and Validation. Customer is responsible for reviewing and validating all Studio Output before relying on it for operational, compliance, legal, financial, customer-facing, or other material purposes.

F4. Workflows, Automation, and Data Freshness

F4.1 Workflow Configuration. Customer is responsible for approving Workflow configuration, inputs, outputs, source systems, destination systems, permissions, schedules, rules, prompts, transformations, and approval gates.

F4.2 Workflow Results. Workflow results depend on Customer Data, data quality, permissions, configurations, third-party systems, and Customer instructions. Redesign is not responsible for errors, omissions, duplication, misclassification, failed routing, incomplete extraction, stale data, or delayed Output caused by Customer Data, Customer Systems, Third-Party Services, or Customer configurations.

F4.3 Data Freshness. Studio Output may reflect Customer Data available at the time of processing and may not reflect later changes to source data, source systems, third-party systems, or Customer configurations. Redesign does not warrant that Studio Output will remain current, complete, or synchronized with any source system.

F4.4 Workflow Changes. Customer shall review changes to Workflows before using them in production or material business processes.

F4.5 No Autonomous High-Risk Use. Customer shall not use Studio Workflows for High-Risk Use or fully automated material decisions without appropriate human review and approval.

F5. Studio Disclaimers

redesign

F5.1 No Accuracy Warranty. Redesign does not warrant that Studio Output will be complete, accurate, error-free, non-duplicative, or suitable for Customer's intended purpose.

F5.2 Unstructured Data Limitations. Customer acknowledges that unstructured data extraction and transformation may be affected by document quality, formatting, handwriting, scans, OCR quality, inconsistent source data, metadata gaps, file corruption, third-party limitations, and Customer configurations.

F5.3 Third-Party Services. Studio may use or connect to Third-Party Services, including third-party models, OCR services, storage environments, analytics tools, and APIs. Redesign is not responsible for Third-Party Services or their output, performance, availability, data handling, security, or changes.

redesign

ADDENDUM G: REDESIGN CLOUD HOSTING SERVICES FOR THE REDESIGN TECHNOLOGY TERMS

This Redesign Cloud Hosting Services Addendum supplements the Technology Terms and governs Customer's access to and use of Redesign's Cloud Hosting Services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). This Addendum applies only if Cloud Hosting Services are included in an Order, enabled for Customer, or otherwise made available by Redesign to Customer.

This Addendum is separate from Addendum B (OpenCloud), which covers Redesign's on-premises private cloud software license. Capitalized terms used but not defined in this Addendum have the meanings given in the Technology Terms or the applicable Order.

PART I: GENERAL PROVISIONS

The following general provisions apply to all Cloud Hosting Services. Service-specific terms are set forth in Part II and supplement these general provisions. In the event of a conflict between Part I and Part II, the service-specific terms control.

G1. DEFINITIONS

Capitalized terms used in this Addendum and not otherwise defined herein have the meanings set forth in the Technology Terms. The following definitions apply to this Addendum:

- (a) "Cloud Hosting Services" means, solely for the purposes of this Addendum, the IaaS Services, PaaS Services, and/or SaaS Services provided by Redesign as specified in the applicable Order.
- (b) "IaaS Services" means infrastructure-as-a-service resources, including virtual machines, compute instances, storage volumes, network resources, and related infrastructure components.
- (c) "PaaS Services" means platform-as-a-service environments, including development tools, runtime environments, middleware, databases, operating systems, and related platform services.
- (d) "SaaS Services" means software-as-a-service applications hosted, operated, and maintained by Redesign and made available to Customer through a web browser, API, or other remote access method.
- (e) "Compute Resources" means virtual machines, compute instances, processing units, CPU cores, memory allocation, and other computational resources.
- (f) "Storage Resources" means block storage, object storage, file storage, backup storage, archival storage, and other data storage resources.
- (g) "Network Resources" means virtual networks, load balancers, firewalls, IP addresses, bandwidth allocation, data transfer capacity, and other networking resources.
- (h) "Development Environment" means the platform infrastructure, tools, libraries, APIs, and services for developing, testing, deploying, and managing applications under PaaS Services.
- (i) "Customer Applications" means software applications, code, scripts, configurations, and related materials developed, deployed, or operated by Customer using PaaS Services.
- (j) "Customer Systems" means virtual machines, operating systems, applications, software, configurations, and other systems deployed, installed, or operated by Customer using IaaS Services.
- (k) "SaaS Application" means the specific Redesign-hosted software application made available to Customer as part of SaaS Services, as identified in the applicable Order.
- (l) "Platform Components" means software, tools, services, APIs, libraries, frameworks, runtime environments, middleware, databases, operating systems, and other components comprising PaaS Services.
- (m) "Hypervisor" means the virtualization layer and associated software enabling the creation, management, and operation of virtual machines and other virtualized infrastructure resources.
- (n) "Service Level Objective" or "SLO" means the service level targets specified in Section G4 or as otherwise set forth in the applicable Order.
- (o) "Subscription Term" means the period during which Customer is authorized to access and use Cloud Hosting Services as specified in the applicable Order.
- (p) "Resource Limits" means the usage limits, capacity restrictions, and consumption thresholds applicable to Customer's use of Cloud Hosting Services as specified in the applicable Order.
- (q) "Critical Failure" means a complete failure of the Cloud Hosting Services that renders the services substantially unusable for their intended purpose.

redesign

- (r) "Maintenance Window" means scheduled periods during which Redesign may perform maintenance that may result in temporary unavailability or reduced performance.
- (s) "User Seats" means the number of individual Authorized Users permitted to access SaaS Services as specified in the applicable Order.

G2. CLOUD HOSTING SERVICE PROVISION

G2.1 Grant of Access. Subject to the terms of the Agreement and the applicable Order, Redesign grants Customer a non-exclusive, non-transferable, non-sublicensable right during the Subscription Term to access and use the Cloud Hosting Services for Customer's internal business purposes, in accordance with the Documentation and applicable Resource Limits. For IaaS Services, and notwithstanding Sections 9(c) and 9(d) of the Technology Terms, Customer may also use the IaaS Services to provide services to its own customers in the ordinary course of business.

G2.2 Service Capabilities. The specific capabilities applicable to each Cloud Hosting Service type are set forth in the applicable Service-Specific Terms in Part II (Sections G.1, G.2, and G.3).

G2.3 Usage Restrictions. In addition to the restrictions set forth in Section 9 of the Technology Terms, Customer shall not, and shall not permit any Authorized User or third party to:

- (a) conduct benchmarking or performance testing of the Cloud Hosting Services without Redesign's prior written consent;
- (b) exceed applicable Resource Limits;
- (c) use Cloud Hosting Services for cryptocurrency mining without Redesign's prior written approval; or
- (d) impose an unreasonable or disproportionately large load on Redesign's infrastructure or engage in activities that may negatively impact other customers.

G2.4 Infrastructure and Platform Updates. Redesign may update, modify, or patch infrastructure and Platform Components from time to time. Redesign will use commercially reasonable efforts to schedule such updates during Maintenance Windows, provide advance notice of material changes, and minimize disruption. For PaaS Services, Redesign will maintain backward compatibility for deprecated Platform Components for not less than ninety (90) days following notice of deprecation.

G2.5 Third-Party Services and Integrations. Section 7 of the Technology Terms applies to Third-Party Services used in connection with the Cloud Hosting Services. Customer's use of Third-Party Services may require Customer to obtain separate licenses or subscriptions.

G3. CUSTOMER DATA, OWNERSHIP, AND PORTABILITY

G3.1 Customer Data Ownership. Customer retains all right, title, and interest in and to Customer Data in accordance with Section 6.1 of the Technology Terms. The license granted to Redesign under Section 6.2 of the Technology Terms applies to Customer Data processed in connection with the Cloud Hosting Services. Redesign's rights to use aggregated, de-identified data are governed by Section 6.5 of the Technology Terms.

G3.2 Customer Applications and Systems Ownership. (a) PaaS: Customer retains all right, title, and interest in Customer Applications. (b) IaaS: Customer retains all right, title, and interest in Customer Systems. (c) SaaS: Customer retains all right, title, and interest in Customer Data and Customer configurations within the SaaS Application.

G3.3 Data Security. Redesign will implement and maintain administrative, technical, and physical safeguards as described in DPA Schedule 2. Security responsibilities are allocated by service type: (a) IaaS: Customer is responsible for all security above the Hypervisor layer; (b) PaaS: Customer is responsible for application-layer security; (c) SaaS: Redesign manages the full application stack, and Customer is responsible for data input and account security.

G3.4 Data Backup. Backup scope, frequency, retention, restoration, and recovery commitments are governed by the applicable Order or Statement of Work. Unless expressly stated otherwise: (a) for IaaS Services, Redesign backs up infrastructure configuration and metadata only, and Customer is responsible for Customer Data and Customer System backups; (b) for PaaS Services, Redesign backs up platform infrastructure, and Customer is responsible for Customer Data, application source code, configurations, and deployment scripts; and (c) for SaaS Services, Redesign maintains backups in accordance with its standard retention schedule. Extended retention or customer-specific backup services may be available for additional fees.

redesign

G3.5 Data Portability. During the Subscription Term, Redesign will provide reasonable export mechanisms enabling Customer to retrieve Customer Data in a standard format. Customer is responsible for exporting Customer Data prior to the expiration or termination of the Subscription Term. To the extent Regulation (EU) 2023/2854 (the EU Data Act) applies to Customer's use of Cloud Hosting Services, Customer's switching and data portability rights under that Regulation supplement this Section G3.5, and Redesign will provide reasonable cooperation with Customer's switching process in accordance with the applicable requirements of the EU Data Act.

G3.6 Data Deletion and Return. Upon expiration or termination of the Subscription Term, data return and destruction will be handled in accordance with the DPA. Customer must export all Customer Data, Customer Applications, and Customer Systems prior to the effective date of termination. Notwithstanding backup residuals, Redesign may delete all remaining Customer Data thirty (30) days after the effective date of termination unless the applicable Order specifies otherwise.

G4. Support and Service Levels

G4.1 Support channels, support hours, response time targets, priority classifications, service level objectives, uptime targets, maintenance windows, and service credits, if any, are as specified in the applicable Order or Statement of Work.

G4.2 Unless the applicable Order specifies otherwise, standard support is available during business hours: 9:00 AM to 6:00 PM Pacific Time, Monday through Friday, excluding US federal holidays. Enhanced support options may be available for additional fees.

G4.3 Redesign may perform scheduled and emergency maintenance that may result in temporary unavailability or reduced performance. Redesign will use commercially reasonable efforts to provide advance notice of scheduled maintenance.

G5. SUBSCRIPTION TERM, RENEWAL, AND TERMINATION

G5.1 Initial Term. The initial Subscription Term for each Cloud Hosting Service shall be as specified in the applicable Order.

G5.2 Renewal. Renewal of the Subscription Term is governed by the applicable Order. Unless the applicable Order specifies otherwise, the Subscription Term automatically renews for successive twelve-month periods unless either Party provides written notice of non-renewal at least sixty (60) days before the end of the then-current Subscription Term.

G5.3 Effect of Termination. Upon the effective date of termination or expiration of the Subscription Term:

- (a) Customer's right to access and use the affected Cloud Hosting Services shall immediately cease, and Redesign shall cease providing such services.
- (b) All Customer Systems and Customer Applications shall become unavailable.
- (c) Customer must export all Customer Data, Customer Applications, Customer Systems, and related materials prior to the effective date of termination using the mechanisms described in Section G3.5.
- (d) Customer Data shall be handled in accordance with Section G3.6 and the DPA.
- (e) Redesign may delete all Customer Data, Customer Applications, and Customer Systems thirty (30) days after the effective date of termination, unless the applicable Order specifies a different retention period.
- (f) All accrued and unpaid payment obligations shall survive termination or expiration.

G6. INTELLECTUAL PROPERTY AND WARRANTIES

G6.1 Redesign Ownership. Redesign, its licensors, and its hosting providers retain their respective rights, title, and interests in the Cloud Hosting Services, infrastructure, Platform Components, SaaS Applications, Hypervisor, management tools, Documentation, and intellectual property embodied therein. No rights are granted to Customer except as expressly stated in this Addendum or the applicable Order.

G6.2 Customer Ownership. Customer retains all right, title, and interest in and to Customer Applications, Customer Systems, Customer Data, and Customer configurations. Redesign acquires no ownership interest except the limited licenses granted under Section G3.

G6.3 Feedback. If Customer provides suggestions, ideas, or feedback regarding the Cloud Hosting Services, Redesign may use such feedback without restriction or obligation to Customer.

redesign

G6.4 Open Source. PaaS Services and SaaS Services may include open source components governed by their respective licenses. For IaaS Services, Customer is solely responsible for obtaining and maintaining licenses for all operating systems, applications, and software deployed on Customer Systems.

G6.5 Performance Warranty. (a) IaaS: the underlying infrastructure will perform materially in accordance with the Documentation and the applicable Order. (b) PaaS: PaaS Services will perform materially in accordance with the Documentation. (c) SaaS: the SaaS Application will perform materially in accordance with the Documentation and the applicable Order during the Subscription Term. Customer must notify Redesign in writing of any claimed nonconformity within thirty (30) days after Customer first becomes aware of it and during the applicable Subscription Term. Failure to provide timely notice constitutes waiver of the warranty claim.

G6.6 Sole Remedy. Redesign will use commercially reasonable efforts to correct any verified nonconformity or provide a reasonable workaround. If correction is not commercially reasonable, Redesign may terminate the affected subscription and refund prepaid, unused fees on a pro rata basis.

G6.7 Customer Systems and Applications Disclaimer. FOR IAAS SERVICES, REDESIGN MAKES NO WARRANTIES REGARDING CUSTOMER SYSTEMS, INCLUDING ANY OPERATING SYSTEMS, APPLICATIONS, OR SOFTWARE INSTALLED OR OPERATED BY CUSTOMER. FOR PAAS SERVICES, REDESIGN MAKES NO WARRANTIES REGARDING CUSTOMER APPLICATIONS OR CUSTOM CODE DEVELOPED, DEPLOYED, OR OPERATED BY CUSTOMER.

G6.8 SaaS Output Disclaimer. SaaS Application output depends on Customer Data quality and Customer configurations. Redesign does not warrant that output will be complete, accurate, error-free, or suitable for Customer's intended purpose.

G6.9 General Disclaimer. The general disclaimers set forth in Sections 13.2, 13.3, and 13.4 of the Technology Terms apply in full to all Cloud Hosting Services. Without limiting the foregoing, Redesign does not guarantee uninterrupted or error-free operation of the Cloud Hosting Services, and Customer acknowledges that Cloud Hosting Services depend on internet connectivity and third-party infrastructure and may be subject to latency, delays, or interruptions inherent in such communications.

G7. SHARED RESPONSIBILITY MODEL AND COMPLIANCE

G7.1 Redesign Responsibilities. Redesign, directly or through its hosting providers, is responsible for the following, as applicable by service type:

- (a) All Cloud Hosting Services: physical security of applicable data center facilities, Hypervisor management and patching, and physical network, storage, and compute infrastructure.
- (b) PaaS Services (in addition to the foregoing): operating systems, middleware, databases, and Platform Components.
- (c) SaaS Services (in addition to the foregoing): the full application stack, application-level security controls, patching, and updates to the SaaS Application.

G7.2 Customer Responsibilities. Customer is responsible for the following, as applicable by service type:

- (a) IaaS Services: everything above the Hypervisor, including operating systems, middleware, applications, data, virtual network configurations, firewalls, access controls, encryption, patching, and compliance.
- (b) PaaS Services: Customer Applications, Customer Data, application-level security, access management, authentication, encryption within applications, and compliance.
- (c) SaaS Services: data input quality and accuracy, account credential security, Authorized User access management, compliance with acceptable use obligations, and review and validation of outputs.

G7.3 Shared Responsibilities. Certain responsibilities are shared between Redesign and Customer: (a) IaaS: network security, where Redesign manages physical network controls and Customer manages virtual network controls; (b) PaaS: identity and access management, where Redesign manages platform-level controls and Customer manages application-level controls; (c) SaaS: data classification, where Redesign maintains infrastructure-level controls and Customer makes data handling and classification decisions.

G7.4 Usage Compliance. Redesign may monitor Customer's use of Cloud Hosting Services for compliance with Resource Limits and the Agreement. If Customer exceeds applicable Resource Limits, Redesign may, at its discretion: (a) invoice Customer for excess usage at then-current rates; (b) require Customer to reduce usage; (c) throttle or limit performance; (d) suspend provisioning of new resources; or (e) suspend access to the affected Cloud Hosting Services upon written notice.

G7.5 Security Audits. Security audit rights are governed by the audit provisions set forth in the DPA.

redesign

G7.6 Compliance Certifications. Redesign's security program is informed by recognized industry standards and frameworks, as described in DPA Schedule 2. No separate certification obligation applies unless expressly stated in the applicable Order.

G8. GENERAL PROVISIONS

G8.1 Multi-Tenancy and Dedicated Environments. Cloud Hosting Services may operate in multi-tenant environments unless the applicable Order expressly identifies a dedicated environment. Where multi-tenant infrastructure is used, Redesign maintains logical separation of Customer Data from other customers' data.

G8.2 API Access and Rate Limits. API access is subject to rate limits, authentication requirements, and Documentation. Redesign may modify APIs upon 90 days prior written notice and will use commercially reasonable efforts to maintain backward compatibility.

G8.3 Beta and Preview Features. Beta or preview features are provided AS IS without warranty and may be modified or discontinued without notice.

G8.4 Service Modifications. Redesign may modify Cloud Hosting Services upon thirty (30) days' advance written notice. If a modification materially diminishes core functionality, Customer may terminate the affected subscription within thirty (30) days after receiving notice and receive a pro rata refund of prepaid, unused fees for the terminated service. Customer remains responsible for accrued fees and any non-cancellable third-party costs, reserved-capacity charges, or other committed amounts identified in the applicable Order.

G8.5 Data Residency. Unless specified in the applicable Order, Customer Data may be stored in the United States or other jurisdictions where Redesign or its subprocessors maintain facilities, subject to the DPA. Specific residency requirements may be available for additional fees.

G8.6 Disaster Recovery. Redesign maintains business continuity and disaster recovery measures per DPA Schedule 2 for underlying infrastructure. Customer is responsible for application-level and system-level disaster recovery.

G8.7 Limitation of Liability. Liability arising under or in connection with this Addendum is governed by Section 14 of the Technology Terms, including the aggregate cap in Section 14.7 and the exclusion of consequential damages in Section 14.8. If the applicable Order expressly modifies Section 14 in accordance with Section 14.9, that modification controls.

G8.8 Survival. Sections G3.6, G5.3, G6, G7, G8.7, and any accrued payment obligations survive expiration or termination of this Addendum or the applicable Subscription Term and any provisions in Part II that by their nature should survive.

PART II: SERVICE-SPECIFIC TERMS

The following Service-Specific Terms supplement the General Provisions set forth in Part I and apply to the specific Cloud Hosting Service types identified below. In the event of a conflict between the General Provisions and any Service-Specific Terms, the Service-Specific Terms shall control with respect to the applicable service type. Each Service-Specific Terms section applies only if the corresponding service type (IaaS, PaaS, or SaaS) is included in the applicable Order, enabled for Customer, or otherwise made available by Redesign to Customer.

SECTION G.1: IAAS-SPECIFIC TERMS

G.1.1 IaaS Service Capabilities. Subject to the applicable Order and Resource Limits, Redesign will provide Customer the ability to: (a) provision and manage Compute Resources, including virtual machines and compute instances; (b) provision and manage Storage Resources; (c) provision and manage Network Resources, including virtual networks, subnets, routing, and security groups; (d) install, configure, and operate Customer Systems, including operating systems, applications, and software of Customer's choice; and (e) scale resources within applicable Resource Limits.

G.1.2 Infrastructure Access and Control. Customer will have full administrative and root access to Customer Systems. Redesign will not access Customer Systems except as necessary to provide infrastructure-level support or as expressly authorized by Customer.

G.1.3 Resource Provisioning. Customer may provision, modify, and deprovision resources through Redesign's management interface, API, or CLI, subject to Resource Limits. Redesign may restrict provisioning in cases of capacity constraints, abuse, or violation of the Agreement.

redesign

G.1.4 Snapshots and Backups. Customer may create snapshots and backups using tools provided by Redesign. Customer is solely responsible for managing, maintaining, and testing all snapshots and backups. Redesign may impose limits on the number, size, and retention period of snapshots and backups.

G.1.5 Network Configuration. Customer may configure virtual networks, subnets, routing tables, and security groups, subject to Redesign's architecture and security requirements. Customer is responsible for proper network configuration and any issues arising from misconfiguration.

G.1.6 IaaS Customer Responsibilities. In addition to Customer's responsibilities under Section G7, Customer is responsible for: (i) selection, installation, configuration, operation, maintenance, security, and performance of Customer Systems; (ii) compliance of Customer Systems with applicable Laws and third-party intellectual property rights; (iii) implementing security controls, access restrictions, authentication, and encryption; (iv) obtaining and maintaining all licenses for operating systems, applications, and software deployed on Customer Systems; (v) monitoring and optimizing resource consumption; (vi) maintaining backups of Customer Data and Customer Systems; (vii) patching, updating, and securing all operating systems, applications, and software; (viii) disaster recovery and business continuity measures for Customer Systems; (ix) ensuring compatibility of Customer Systems with the underlying infrastructure; (x) installing, configuring, and maintaining firewalls, intrusion detection systems, and antivirus software; (xi) logging, monitoring, and alerting within Customer Systems; (xii) managing user access, authentication, and authorization; (xiii) conducting security assessments and vulnerability scans of Customer Systems; and (xiv) responding to security incidents affecting Customer Systems.

G.1.7 Redesign Responsibilities (IaaS). In addition to Redesign's responsibilities under Section G7, Redesign will: (a) maintain the underlying infrastructure, including physical servers, storage hardware, and network equipment; (b) apply security patches to the Hypervisor and infrastructure components; (c) monitor infrastructure performance, availability, capacity, and security; (d) maintain physical security, power, cooling, and environmental controls at data center facilities; (e) maintain network-level security controls for the physical network; and (f) provide provisioning, management, and monitoring tools.

G.1.8 Licensing Compliance. Customer is solely responsible for obtaining, maintaining, and complying with all license terms for software deployed on or used in connection with Customer Systems. Customer shall indemnify and hold harmless Redesign from and against all Losses arising from or related to any third-party licensing claims associated with Customer Systems.

SECTION G.2: PAAS-SPECIFIC TERMS

G.2.1 PaaS Service Capabilities. Subject to the Agreement and the applicable Order, Customer may: (a) develop, test, deploy, and manage Customer Applications using the Development Environment; (b) utilize Platform Components, including runtime environments, middleware, databases, and development tools; (c) store and process Customer Data within PaaS Services; (d) configure and customize the platform within Redesign's published parameters; (e) integrate with third-party services and APIs, subject to applicable restrictions; and (f) monitor, analyze, and optimize performance using provided tools.

G.2.2 Customer Responsibilities (PaaS). Customer is solely responsible for: (i) development, testing, functionality, performance, security, and operation of Customer Applications; (ii) compliance of Customer Applications with applicable Laws and third-party intellectual property rights; (iii) application-level security controls, authentication, and access restrictions; (iv) monitoring and optimizing resource consumption; (v) maintaining backups of source code, configurations, and deployment scripts; (vi) compatibility with Platform Components and managing the impact of platform updates; (vii) error handling, logging, and monitoring within Customer Applications; (viii) managing application dependencies, libraries, and third-party integrations; (ix) application-level security, including input validation, output encoding, and protection against common vulnerabilities; (x) security testing and vulnerability assessments of Customer Applications; and (xi) end-user support for Customer Applications.

G.2.3 Redesign Responsibilities (PaaS). In addition to the responsibilities set forth in Section G8, Redesign will: (a) apply security patches to operating systems, middleware, databases, and Platform Components; (b) maintain underlying compute, storage, and network infrastructure supporting the platform; and (c) provide development, deployment, and monitoring tools as described in the Documentation.

G.2.4 Development and Production Environments. Customer may create multiple environments (e.g., development, testing, staging, production) subject to Resource Limits specified in the applicable Order. Customer is responsible for maintaining appropriate separation and security controls between environments.

redesign

G.2.5 Platform Dependencies. Customer Applications may depend on specific Platform Component versions. Redesign will use commercially reasonable efforts to maintain availability of Platform Components but may deprecate or discontinue components upon not less than 90 days prior written notice. Customer is responsible for monitoring deprecation notices and updating Customer Applications accordingly. Redesign will use commercially reasonable efforts to maintain backward compatibility for deprecated components during the notice period.

SECTION G.3: SAAS-SPECIFIC TERMS

G.3.1 SaaS Service Description. Redesign will host, operate, and maintain the SaaS Application identified in the applicable Order and make it available to Customer and its Authorized Users during the Subscription Term via web browser, API, or other remote access method specified in the Documentation.

G.3.2 SaaS Access Rights. Access is limited to the number of User Seats, features, modules, storage capacity, and usage volumes specified in the applicable Order. Customer may not exceed User Seats or share credentials. Each Authorized User must have a unique account.

G.3.3 SaaS Service Capabilities. Customer may: (a) access and use the SaaS Application for internal business purposes; (b) store, process, and retrieve Customer Data; (c) configure the SaaS Application within available parameters; (d) generate reports and outputs using available functionality; and (e) integrate with supported third-party services as documented.

G.3.4 Redesign Responsibilities (SaaS-Specific). Redesign will: (i) host, operate, and maintain the SaaS Application and underlying infrastructure; (ii) apply security patches and updates to the full application stack; (iii) monitor performance, availability, capacity, and security; (iv) maintain logical separation of Customer Data in multi-tenant environments; (v) provide application-level access controls, authentication, and authorization mechanisms; (vi) maintain backups per Redesign's standard retention schedule; and (vii) implement application-level security controls, including input validation, encryption, and session management.

G.3.5 Customer Responsibilities (SaaS-Specific). Customer is responsible for: (i) accuracy, quality, legality, and appropriateness of Customer Data entered into the SaaS Application; (ii) maintaining confidentiality of account credentials, passwords, API keys, and access tokens; (iii) managing Authorized User accounts, permissions, and access; (iv) reviewing and validating output before relying on it for material decisions; (v) compliance with acceptable use policies and applicable Laws; (vi) configuring and maintaining integrations with third-party services; and (vii) promptly notifying Redesign of any unauthorized use or security concerns.

G.3.6 SaaS Updates and Modifications. Redesign may update, modify, or deprecate SaaS Application features. Redesign will use commercially reasonable efforts to provide advance notice of material changes that may adversely affect Customer's use. Certain updates may change functionality, user interfaces, or workflows. Redesign has no obligation to maintain prior versions following release of updates.

G.3.7 SaaS Data Processing. Customer authorizes Redesign to access, process, store, and transmit Customer Data as necessary to provide the SaaS Services. Redesign will not access Customer Data except as necessary to: (a) provide, secure, support, maintain, and administer the SaaS Application; (b) investigate and resolve issues; (c) comply with applicable Law; (d) enforce the Agreement; or (e) exercise rights expressly authorized under Section 6.7.

G.3.8 SaaS Availability. Redesign will use commercially reasonable efforts to make the SaaS Application available on a continuous basis, subject to Maintenance Windows, the Agreement, and any availability terms and exclusions stated in the applicable Order. Redesign is not responsible for unavailability caused by Customer's internet connectivity, equipment, browser compatibility, third-party integrations, or actions of Authorized Users.

G.3.9 User Seat True-Up. If Customer exceeds the number of User Seats specified in the applicable Order, Redesign may invoice Customer for the additional User Seats at Redesign's then-current rates or the rates stated in the applicable Order, whichever is specified therein.

G.3.10 SaaS-Specific Disclaimers. (i) Redesign does not warrant that the SaaS Application will meet Customer's specific requirements or integrate with all Customer systems or third-party services. (ii) Features, functionality, and availability may vary by subscription tier and geographic region. (iii) The SaaS Application may contain features that use AI or machine learning; output from such features may be incomplete, inaccurate, or unsuitable for Customer's intended purpose, and Customer is responsible for reviewing all such output before reliance. (iv) Customer acknowledges that SaaS Services depend on internet connectivity and third-party infrastructure and may be subject to latency, delays, or interruptions inherent in such communications.

redesign

The Redesign Group | 222 N Pacific Coast Hwy, Floor 10, El Segundo, CA 90245, United States | redesign-group.com