Managed Digital Risk Monitoring (MDRM) Product Terms

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms apply when Customer purchases Rackspace Managed Digital Risk Monitoring (the **"Services"** or **"MDRM"**). Capitalized terms used but not defined in these Product Terms have the meanings given in the Agreement.

1. ADDITIONAL DEFINED TERMS.

"Coverage Hours" means 24 hours per day, 7 days per week, year-round, being the window during which Rackspace monitors the Covered External Assets and measures the Service Levels in Section 8, unless otherwise stated in the Service Order.

"Covered External Assets" or **"Monitored Assets"** means the Customer-owned or Customer-designated external-facing assets documented as within scope of the Services during onboarding, which may include domains, subdomains, watchwords, email addresses, brand names and trademarks, source code repositories, API endpoints and tokens, storage buckets, BIN ranges, IP ranges, employee or executive identities, social media handles, and official application identifiers.

"Designated Customer Contact" means a Customer contact authorized, on Customer's behalf, to submit and manage support tickets, submit policy and escalation requests, approve Takedown actions, and interface with Rackspace regarding the Services.

"Detection" means the time at which a potential Exposure first becomes available to Rackspace through the Supported Platform or a Third-Party Source.

"Exposure" means a validated instance of Customer-related data, credentials, brand impersonation, or other material risk identified in external sources, including the deep and dark web, open repositories, data-dump sites, and public platforms.

"Exposure Report" means a structured report identifying the source of an Exposure, the matched Covered External Assets, analyst commentary, and recommended remediation steps.

"Letter of Authorization" or **"LOA"** means a written authorization, in a form acceptable to Rackspace and any applicable third party, by which Customer authorizes Rackspace to request a Takedown on Customer's behalf.

"Magnitude" means the classification (High, Medium, or Low) assigned by Rackspace to indicate the severity and potential impact of a validated Exposure for triage and Service Level purposes, as described in Section 8.

"**Platform Provider**" means CloudSEK Research PTE. LTD. ("**CloudSEK**") and any other third party that provides the Supported Platform or any Third-Party Source.

"Platform Terms" means the Platform Provider's terms applicable to the Supported Platform, including any end-user license agreement, acceptable-use policy, and data-processing terms, as Rackspace makes available to Customer during onboarding or on request.

"Rackspace Cyber Defense Center" or **"RCDC"** means the Rackspace service hub for managed security services, including the Rackspace security operations analysts who deliver the Services.

"Supported Platform" means CloudSEK's XVigil digital risk protection and external attack surface monitoring platform and associated tooling, together with the Third-Party Sources, that Rackspace uses to deliver the Services, as Rackspace may select, supplement, or change from time to time.

© 2026 Rackspace US, Inc. – Global Product Terms – July 30, 2026 Revision – OT# 60369

“Takedown” means a request for the removal, disruption, or de-indexing of infringing or malicious external content or infrastructure, subject to third-party acceptance and the requirements in Section 4.

“Third-Party Sources” means the third-party data sources, feeds, intelligence, and platforms used to deliver the Services, including (as applicable) deep and dark web feeds, breach compilation sources, marketplaces, messaging platforms, public code repositories, cloud storage discovery, app-store monitoring, and social platforms.

2. OVERVIEW. Rackspace Managed Digital Risk Monitoring is a managed security service that proactively monitors external threat vectors outside Customer’s environment, validates exposures relating to the Covered External Assets, and supports mitigation and Takedown activity. MDRM is intended to reduce Customer’s exposure to data leaks, credential theft, and brand abuse by continuously monitoring external sources such as the deep and dark web, open repositories, and brand-related channels. The Services combine the Supported Platform with Rackspace security operations analysts who validate findings, assess impact, and provide Exposure Reports, remediation guidance, and Takedown assistance where applicable. The Services monitor sources external to Customer’s environment and are not a monitoring, detection, or response service for Customer’s own systems, networks, or endpoints.

3. THE MDRM SERVICES.

3.1. Deployment and Onboarding Services.

(A) Kick-off. Rackspace will provide initial onboarding and orient Customer to the MDRM support model. The deployment plan, key milestones and deliverables, and the Designated Customer Contacts will be reviewed and agreed by the parties.

(B) Asset Onboarding and Discovery. The parties will conduct discovery to establish MDRM coverage. Customer will provide an initial asset inventory and points of contact so that the Monitored Assets are accurately captured. Supported asset types include domains and subdomains, email addresses, brand names, trademarks, watchwords, BIN ranges, source code repositories, API endpoints and tokens, storage buckets, employee and executive identities, social media handles, and official application identifiers.

(C) Source Integration and Coverage Configuration. Rackspace will configure the Supported Platform and monitoring coverage to include, as applicable, deep and dark web feeds, breach compilation sources, marketplace coverage, messaging platforms (e.g., forums, Telegram, Discord, IRC), public code repositories, cloud storage discovery, app-store monitoring, and social platforms.

(D) Matching and Correlation Rules. Rackspace will configure matching and correlation rules to identify Customer-related Exposures (e.g., credential matches, brand variants, BIN patterns, repository and API-key detections), with context enrichment where available.

(E) Additional Asset Onboarding. If Customer introduces additional assets into the Covered External Assets after initial implementation, Rackspace will evaluate whether they can be accommodated within the existing monitoring design; where customization or additional discovery is required, additional Fees may apply.

(F) Validation and Sign-off. The parties will hold a validation workshop to confirm that coverage has been configured and that asset inventories and watchwords are current. Rackspace will inform Customer when MDRM has been enabled.

3.2. Ongoing Managed Services. Following onboarding, the RCDC will perform the following ongoing managed Services for the Covered External Assets:

(A) Continuous Monitoring. Rackspace will monitor external threat landscapes (including the deep and dark web, open repositories, app stores, and social channels) for Customer-related Exposures.

(B) Analyst Validation. Rackspace security operations analysts will validate potential findings prior to escalation, including evidence collection and context assessment.

(C) Exposure Reporting. Rackspace will deliver Exposure Reports identifying source details, matched assets, analyst commentary, and recommended remediation steps.

(D) Notifications and Integrations. Notifications may be delivered by email or, where agreed with Customer, through integrated platforms such as Rackspace Managed XDR.

(E) Takedown Facilitation. Where findings involve external content or infrastructure, Rackspace can facilitate Takedown support under Section 4, subject to Customer authorization and third-party acceptance. Takedown facilitation is included up to the Takedown allowance set out in the Service Order; additional Takedowns are subject to an additional Fee.

(F) Attack Surface Visibility. Rackspace will make available dashboards summarizing Monitored Assets, exposure categories and counts, validation status, Takedown status, and trends.

(G) Innovation and Enhancements. On a quarterly basis, Rackspace will review the evolving threat landscape and may recommend new watchwords, additional coverage, or detection enhancements. Where an enhancement could materially affect the Services, Rackspace will notify Customer.

(H) Platform Support. Designated Customer Contacts will have access to ticket-based support through the Rackspace portal and to support by email for MDRM platform and support requests.

3.3. Module Capabilities and Analyst Response. The following MDRM modules and associated analyst-response activities are included in the Services; prioritization and Service Levels are described in Section 8.

(A) Deep and Dark Web Monitoring. Monitoring covers (i) credential breaches (combination lists) — leaked usernames and passwords tied to the Covered External Assets; (ii) compromised computers and malware logs — stealer-malware logs containing credentials, cookies, and system fingerprints; (iii) dark web marketplaces offering stolen credentials and identities; and (iv) dark web discussions across forums and messaging channels (e.g., Telegram, Discord, IRC) referencing Customer. Analyst response: validate the Exposure and provide matched evidence; advise on credential reset and MFA enforcement; advise on endpoint remediation for malware-infected systems; and deliver validated Exposure Reports with impact commentary.

(B) Data Leak Monitoring. Monitoring covers (i) code repositories — exposed source code, API keys, or credentials; (ii) compromised computers — stealer-malware data leaks tied to Customer subdomains or accounts; (iii) leaked documents and open buckets — misconfigured cloud storage and public file-sharing; (iv) API platforms — exposed keys, tokens, or internal endpoints; and (v) payment-card leaks — BIN-based card data offered for sale. Analyst response: recommend key and token revocation and regeneration; provide remediation steps for misconfigured storage; advise on notification of financial institutions for card exposures where appropriate; and deliver repository-hygiene recommendations.

(C) Brand Risk Monitoring. Monitoring covers (i) fake domains and phishing sites — lookalike or typo-squatted domains impersonating Customer; (ii) fake mobile apps — rogue applications in official or third-party app stores; (iii) fake social media handles and pages — fraudulent accounts impersonating the brand; (iv) fake call centers — fraudulent numbers and scams posing as Customer support; and (v) social media discussions — misinformation and impersonation-related activity. Analyst response: upon Customer confirmation, initiate Takedown requests for domains, apps, or social accounts; provide advisories for Customer communications where end customers may be affected; and deliver validated Exposure Reports with mitigation steps.

(D) Alerting and Incident Handling. Findings are validated prior to escalation and classified by Magnitude. Magnitude classifications and validation determinations are analyst assessments made on the basis of information available from the Supported Platform and Third-Party Sources (see Section 12). Exposure Reports include evidence, matched assets, analyst commentary, and remediation steps. Notifications are provided under Section 3.2 and as agreed with Customer.

3.4. Remediation Guidance and Coordination. Rackspace will provide remediation guidance consistent with the Exposure type, which may include credential resets and MFA enforcement, revocation and regeneration of keys and tokens, repository-hygiene improvements, storage-bucket reconfiguration, and advisories for Customer communications. For Customer-managed environments or third-party-controlled platforms, Rackspace will advise on next steps and, where appropriate and authorized, coordinate notifications with relevant third parties (e.g., financial institutions). Remediation within Customer's own systems and environments is the responsibility of Customer.

3.5. Service Reviews and Reporting. Rackspace will deliver operational reporting and periodic service reviews covering service health, notification responsiveness, exposure trends, and watchword and coverage recommendations, on the cadence set out in Section 8 or the Service Order. The specific report content and use-cases will be agreed between the parties.

3.6. Service Exclusions. The Services do not include, and Rackspace has no obligation to provide: (a) monitoring, detection, or response for Customer's own systems, networks, endpoints, or internal environment; (b) forensic analysis or forensic reporting; (c) data recovery; (d) incident-response retainer services; (e) legal services or legal representation; or (f) crisis management or business-service-restoration activities. Takedown-specific exclusions are in Section 4.4.

4. TAKEDOWN SUPPORT.

4.1. Scope. Takedown support applies to phishing and impersonating domains, fake applications, rogue repositories, impersonating social media accounts, and similar abuses of Customer's brand or assets.

4.2. Requirements. As a condition of Takedown support, Customer must provide an LOA, required trademark or ownership documentation, and any additional materials requested by platform providers or hosting entities to substantiate the request.

4.3. Process and Escalation. Upon Customer authorization, Rackspace will prepare and submit Takedown requests to the relevant platform or hosting providers. If a request is rejected, Rackspace will continue escalation with hosting providers and other available channels until reasonable options are exhausted. Takedown outcomes depend on third-party platforms, hosting providers, and registrars and cannot be guaranteed.

4.4. Exclusions. Takedown support excludes domain-ownership disputes and matters requiring UDRP/INDRP or other legal resolution; defamation claims without impersonation or phishing intent; fair-use matters (e.g., commentary, criticism, research); and broader legal disputes outside Takedown eligibility criteria.

4.5. Authorization and Indemnity. Rackspace prepares and submits Takedown requests in reliance on Customer's authorization and the representations in Section 6.2, and acts at Customer's direction in doing so. Customer's indemnification obligations under the Agreement extend to any third-party claim arising from a Takedown requested or authorized by Customer, including any claim by the target of a Takedown.

5. DELIVERABLES. The Services include the following deliverables, as applicable: (a) validated alerts mapped to the Covered External Assets; (b) Exposure Reports including evidence and analyst commentary; (c) remediation guidance tailored to the Exposure type; (d) Takedown tracking with case updates and closure confirmation, where applicable; and (e) operational and executive-level reporting.

6. CUSTOMER OBLIGATIONS AND DEPENDENCIES. Rackspace's performance of the Services, and the applicable Service Levels, are conditioned on Customer's performance of the obligations in this Section. Rackspace is not liable for any failure, delay, or impairment of the Services, and no Service Level credit is due, to the extent caused by Customer's failure to meet them.

6.1. Asset Inventory and Scope. Customer is responsible for providing and maintaining an accurate and complete inventory of the Covered External Assets, watchwords, and identifiers, and for promptly notifying Rackspace of additions or changes. Rackspace has no obligation to monitor assets not documented as Covered External Assets and shall have no liability for Exposures relating to assets, watchwords, or identifiers that Customer has not provided.

6.2. Authorizations. Customer is responsible for providing the LOA, trademark and ownership documentation, and other authorizations required for Takedown and remediation coordination, and represents and warrants that it is authorized to designate the Covered External Assets for monitoring and to request Takedowns in respect of them.

6.3. Designated Contacts and Approvals. Customer is responsible for designating and keeping current the Designated Customer Contacts and for providing timely approvals, authorizations, and information that the Services require. Customer acknowledges that delays in approval or response may delay validation, notification, Takedown, or remediation.

6.4. Remediation. Customer is responsible for implementing remediation within its own systems and environments, including credential resets, key and token revocation, and configuration changes; Rackspace's role is limited to guidance and, where authorized, third-party coordination.

6.5. Lawful Use. Customer is responsible for ensuring that its designation of Covered External Assets, watchwords, and identifiers, and its use of the Services and any Exposure data, comply with applicable law, including data protection and privacy law, and do not infringe the rights of any third party.

6.6. General Cooperation. Customer will provide the cooperation, access, information, and authorizations reasonably required for the Services, including for onboarding. To the extent Customer does not do so: (i) Rackspace is excused from its dependent obligations; (ii) Rackspace may invoice Customer for additional costs or expenses reasonably resulting from the non-cooperation; and (iii) if the failure continues for ninety (90) days or more, Rackspace may commence the service term and begin charging the recurring Fee.

7. SUPPORTED PLATFORM AND THIRD-PARTY SOURCES.

7.1. Third-Party Platform. The Services are delivered using the Supported Platform and Third-Party Sources, which are provided by one or more Platform Providers. Customer acknowledges that the Platform Providers, not Rackspace, are responsible for the features, functionality, coverage, availability, and performance of the Supported Platform and Third-Party Sources, and that a Platform Provider may modify, update, suspend, or discontinue the Supported Platform or any Third-Party Source, which may affect the scope or delivery of the Services.

7.2. Platform Terms; Pass-Through. Customer's access to and use of the Supported Platform is subject to the Platform Terms, including the CloudSEK End User License Agreement (the "CloudSEK EULA"). Rackspace will make the Platform Terms available to Customer at or before onboarding and on request. By purchasing, accessing, or using the Services, Customer agrees to comply, and to ensure its Authorized Users comply, with the Platform Terms as a condition of receiving the Services. The Platform Provider is an intended third-party beneficiary of this Section 7.2 and Section 7.3 and may enforce them directly against Customer.

7.3. Platform Use Restrictions. Customer will not, and will not permit its Authorized Users to: (a) use the Supported Platform other than for Customer's internal business purposes in connection with the Services; (b) copy, modify, republish, or create derivative works of the Supported Platform; (c) reverse engineer, decompile, or disassemble the Supported Platform, except to the extent applicable law prohibits this restriction; (d) use the

Supported Platform to develop or assist in developing a competing product or service, or copy any of its features, functions, or graphics; (e) use the Supported Platform to run automated queries against external websites or systems; (f) interfere with or disrupt the integrity or performance of the Supported Platform; (g) attempt to gain unauthorized access to the Supported Platform or its related systems or networks; (h) remove or alter any proprietary notice on the Supported Platform; (i) perform penetration or load testing of the Supported Platform without Rackspace's and the Platform Provider's prior written consent; or (j) conduct any public benchmarking or comparative analysis of the Supported Platform without prior written consent.

7.4. Limited Rackspace Obligation. Rackspace's obligations on any matter dependent on a Platform Provider or Third-Party Source (including source coverage, feed latency or availability, platform availability, and Takedown acceptance) are limited to using commercially reasonable efforts to obtain the relevant third party's performance, and Rackspace is not liable for a Platform Provider's or Third-Party Source's acts, omissions, or failure to perform. Any service levels, warranties, or indemnities relating to the Supported Platform or a Third-Party Source are provided (if at all) by the applicable Platform Provider and are not service levels, warranties, or indemnities of Rackspace.

7.5. Conflicts. In the event of a conflict between these Product Terms and the Platform Terms with respect to Customer's use of the Supported Platform, the Platform Terms prevail as to that use; with respect to the managed Services performed by Rackspace, these Product Terms prevail.

7.6. Vendor-Driven Service Change. If a Platform Provider discontinues or materially changes the Supported Platform or a Third-Party Source, or revokes or materially restricts Rackspace's access to or rights in it, and the effect renders the affected Services commercially impracticable or operationally unworkable for Rackspace and Rackspace cannot reasonably remediate or work around it, then Rackspace may, on reasonable prior written notice, suspend, de-scope, transition to an alternative source or platform, or terminate the affected Services, and no such action is a breach of these Product Terms or the Agreement. Where Rackspace terminates the affected Services under this Section 7.6 for a cause not attributable to Customer, Customer's sole and exclusive remedy is a pro-rata refund or credit of pre-paid, unused recurring Fees for the period after termination.

8. SERVICE LEVELS. Service Levels are measured during Coverage Hours, apply to validated Exposures and related activity as set out below, and are Rackspace's own managed-service commitments measured from Detection — not commitments regarding the Supported Platform or any Third-Party Source (see Section 7). The Service Credits in this Section are Customer's sole and exclusive remedy for any failure to meet the Service Levels.

8.1. Magnitude Definitions.

(A) High. A clear and active risk to Customer (e.g., a verified credential compromise with current access potential; an active phishing domain or fake application; exposed keys or tokens granting access; or confirmed malware logs tied to Customer identities or systems).

(B) Medium. A likely material risk requiring timely action (e.g., repository exposure of non-critical secrets; a dormant lookalike domain with phishing indicators; or previously exposed credentials requiring hygiene enforcement).

(C) Low. A lower-immediacy or indirect risk (e.g., brand mentions with negative sentiment but no impersonation; or stale exposures with low exploitation likelihood).

8.2. Service Targets.

Activity	Target
Validation of High-Magnitude Exposures	Within 60 minutes of Detection
Validation of Medium-Magnitude Exposures	Within 4 hours of Detection
Validation of Low-Magnitude Exposures	Within 24 hours of Detection

Activity	Target
Incident notification to Customer	Within 1 hour of validation (High); 4 hours (Medium); 24 hours (Low)
Takedown submission	Within 7 Business Days of Customer authorization and receipt of a complete LOA and required documentation
Operational reporting	Weekly summaries of validated alerts and incidents
Executive reporting	Monthly exposure trends and service overview

8.3. Service Credits. If Rackspace fails to meet a validation or notification Target in Section 8.2 (each, a **"Qualifying Failure"**), Customer may request a Service Credit equal to two and one-half percent (2.5%) of the monthly recurring Fee for the Services for the affected month per Qualifying Failure, up to a maximum of ten percent (10%) of that monthly recurring Fee in any calendar month. Service Credits are calculated and applied in accordance with the Agreement.

8.4. Service Level Exclusions. No Service Credit is due, and a Target is not failed, to the extent the relevant delay or failure arises from or relates to: (a) the latency, coverage, availability, or non-performance of any Supported Platform, Third-Party Source, or Platform Provider; (b) third-party acceptance, rejection, or timing of a Takedown; (c) Customer's failure to meet its obligations in Section 6 (including incomplete or inaccurate asset inventories, watchwords, authorizations, or documentation, or delayed approvals); (d) Maintenance, or suspension of the Services in accordance with the Agreement; (e) any matter excluded under Sections 3.6, 4.4, or 7; or (f) any circumstance outside Rackspace's reasonable control, including those described in the force-majeure provisions of the Agreement. The Takedown-submission, operational-reporting, and executive-reporting items in Section 8.2 are operational targets only and do not carry a Service Credit.

8.5. Credit Requests; Cap; Non-Cumulative. Customer must request a Service Credit in writing via a support ticket within seven days after the event giving rise to it. Time-based measurements are determined by Rackspace's ticketing and monitoring systems. Approved Service Credits are applied to invoices issued after approval and are not refundable. Customer is not eligible for a Service Credit if Customer is in breach of the Agreement (including its payment obligations) when the event occurs. If a single event gives rise to more than one Service Credit, only the largest applies, and the Service Credits under this Section are subject to the aggregate SLA credit cap in the Agreement.

9. FEES, TERM, AND TERMINATION.

9.1. Fees. Customer will pay the Fees stated in the Service Order. Unless the Service Order states otherwise, the Services comprise: (a) a one-time onboarding and implementation Fee, invoiced on execution of the Service Order; (b) a monthly recurring Fee for the ongoing managed Services, based on the subscription tier set out in the Service Order, where the tier reflects the number of Covered External Assets monitored and the modules and coverage selected; (c) Takedown facilitation, which is included up to the allowance set out in the Service Order, with additional Takedowns charged as set out there; and (d) any additional or pass-through charges, invoiced as incurred. For fee purposes, Covered External Assets are counted as set out in the Service Order (for example, by domain, subdomain, IP address, watchword, executive identity, and logo), subject to any minimum number of Covered External Assets stated in the Service Order. All Fees are payable in accordance with the Agreement.

9.2. Indexation. Notwithstanding the Agreement, Rackspace may increase the Fees for the Services with effect on or after each anniversary of the initial Service Order by up to the greater of five percent (5%) or the indexation published at https://www.rackspace.com/information/legal/indexation.

9.3. Term. The initial term is as stated in the Service Order and corresponds to the underlying platform subscription term. The Services renew in accordance with the Agreement. Following expiry of the initial term, the End of Life Terms apply to the Services.

9.4. Termination Effects. On expiry or termination, Rackspace will cease the Services, cease monitoring the Covered External Assets, close or hand off open Takedown cases to the extent practicable, and handle Customer Data in accordance with the Agreement and any applicable Data Processing Addendum. Customer is responsible for retaining its own records; following termination, Customer's access to the Supported Platform and to any platform-hosted data ceases, and such data may not be retrievable. Customer remains responsible for Fees accrued through the effective date of termination.

10. DATA PROTECTION, SECURITY, AND COMPLIANCE.

10.1. Data Protection. Where Rackspace's provision of the Services involves processing Customer personal data subject to data protection law, that processing is governed by the Data Processing Addendum incorporated into the Agreement. The Platform Provider may process Customer personal data as a sub-processor under, and any cross-border transfer is governed by, the Data Processing Addendum. Customer acknowledges that Exposure data identified by the Services may include personal data relating to Customer's personnel or to third parties (for example, leaked credentials or identifiers), that Rackspace processes such data solely to provide the Services, and that Customer is responsible for ensuring it has a lawful basis for the monitoring it directs and for the watchwords and identifiers it designates.

10.2. Security. Rackspace maintains the security measures set out in the Global Security & Privacy Practices and the Technical and Organizational Measures, as applicable to the Services. The Supported Platform is maintained by the Platform Provider under its own security program.

10.3. Acceptable Use. Customer will comply, and cause its users to comply, with the Acceptable Use Policy; failure to do so is a material breach, and Rackspace may suspend the Services in accordance with the Agreement.

10.4. Healthcare. The Services are not a HIPAA-Eligible Service, and Customer will not provide protected health information to Rackspace in connection with the Services.

10.5. Export and Sanctions. Customer will not use the Services in violation of applicable export control or economic sanctions laws, and the Services are available only in the territories Rackspace designates in the Service Order.

10.6. Compliance Responsibility. Rackspace makes no representation or warranty that the Services will meet or maintain Customer's legal or regulatory requirements. Customer is responsible for determining whether, and using the Services so that, they meet Customer's legal and regulatory requirements applicable to Customer's use.

11. WARRANTIES, DISCLAIMERS, AND LIMITATION OF LIABILITY.

11.1. Service Warranty. Rackspace warrants that it will perform the Services in a professional and workmanlike manner consistent with generally accepted industry standards. This warranty applies solely to the managed Services performed by Rackspace and does not extend to the Supported Platform, any Third-Party Source, or any Platform Provider, or to the results or outcomes of monitoring or Takedown.

11.2. DISCLAIMER. EXCEPT AS EXPRESSLY STATED IN SECTION 11.1 AND THE AGREEMENT, THE SERVICES ARE PROVIDED "AS IS," AND RACKSPACE DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THE SUPPORTED PLATFORM AND THIRD-PARTY SOURCES ARE PROVIDED BY THE PLATFORM PROVIDER ON AN "AS IS" AND "AS AVAILABLE" BASIS. RACKSPACE DOES NOT WARRANT THAT THE SERVICES WILL DETECT ALL EXPOSURES, THAT MONITORING WILL BE UNINTERRUPTED OR ERROR-FREE, THAT ANY EXPOSURE WILL BE CAPABLE OF REMEDIATION, OR THAT ANY TAKEDOWN WILL SUCCEED.

11.3. Limitation of Liability. Rackspace's liability arising out of or relating to the Services is governed by, and subject to, the limitations and exclusions of liability in the Agreement.

12. CUSTOMER ACKNOWLEDGEMENTS. Customer acknowledges and agrees that:

(1) the Services monitor sources external to Customer's environment and are not a substitute for security monitoring, detection, or response within Customer's own systems, networks, or endpoints;

(2) external monitoring is inherently incomplete and depends on the coverage of Third-Party Sources, which evolves over time and is not exhaustive; Rackspace cannot detect, and does not warrant detection of, all Exposures, and the absence of a finding is not assurance that an Exposure does not exist;

(3) Takedown outcomes depend on third parties and cannot be guaranteed, and Rackspace's obligation is limited to submission and reasonable escalation under Section 4;

(4) the Services do not prevent, and Rackspace does not warrant immunity from, data breaches, credential theft, brand abuse, or other security or reputational harm;

(5) the effectiveness of the Services depends on the accuracy and completeness of the Covered External Assets, watchwords, and identifiers Customer provides and on Customer's timely approvals and remediation;

(6) the Services are provided for Customer's commercial use and must not be used in any situation where failure or fault of the Services could lead to death or serious bodily injury or to physical or environmental damage;

(7) findings, validation determinations, and Magnitude classifications are analyst assessments made on the basis of available information, may include false positives or false negatives, and Customer is responsible for its own decisions and for any action it takes or declines to take in response to an Exposure Report, alert, notification, or guidance; and

(8) the Services are delivered using a third-party Supported Platform and Third-Party Sources, and the modification, suspension, discontinuation, or non-performance of the Supported Platform or any Third-Party Source by a Platform Provider may affect the Services.

13. CHANGES TO PRODUCT TERMS. Notwithstanding anything in the Agreement to the contrary, Rackspace may change these Product Terms in response to (a) changes in applicable law; (b) changes to a Platform Provider, Supported Platform, or Third-Party Source on which the Services depend, or to their governing terms; or (c) operational changes generally applicable to customers or reasonably required, in Rackspace's reasonable determination, for the ongoing performance or proper functioning of the Services. Changes take effect on the earlier of any applicable third-party or legal effective date, posting by Rackspace, or notice to Customer.