Randori Platform Terms of Service

Cloud Services Agreement

THIS CLOUD SERVICES AGREEMENT AND ATTACHED SERVICE DESCRIPTION (TOGETHER, THE AGREEMENT) GOVERNS THE USE OF THE RANDORI PLATFORM, HOWEVER IN THE EVENT OF CONFLICT THIS AGREEMENT IS SUPERSEDED BY ANY OTHER AGREEMENT ENTERED INTO BETWEEN RANDORI AND CLIENT, AND IS NOT APPLICABLE TO AN IBM CLIENT THAT PURCHASED ENTITLEMENTS TO ACCESS IBM SECURITY RANDORI RECON THROUGH IBM.

PLEASE READ THIS CAREFULLY BEFORE ATTEMPTING TO ACCESS OR USE THE RANDORI PLATFORM. THIS AGREEMENT CONSTITUTES A LEGALLY BINDING AGREEMENT BETWEEN YOU OR THE COMPANY WHICH YOU REPRESENT AND ARE AUTHORIZED TO BIND (THE "CLIENT" OR "YOU"), AND RANDORI, INC. ("RANDORI" OR "WE"). THIS AGREEMENT GOVERNS YOUR ACQUISITION AND USE OF THE RANDORI PLATFORM AND RELATED OFFERINGS. PLEASE ONLY CREATE A SERVICE ACCOUNT OR OTHERWISE USE THE PLATFORM OR ANY RELATED OFFERINGS IF YOU AGREE TO BE LEGALLY BOUND BY ALL TERMS AND CONDITIONS HEREIN. BY ACCEPTING THIS AGREEMENT, BY (1) CREATING A SERVICE ACCOUNT AND USING THE PLATFORM OR RELATED OFFERINGS, (2) EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR (3) USING TRIAL SERVICES (WHETHER PURSUANT TO AN EVALUATION AGREEMENT OR OTHERWISE), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH ANY ASPECT OF THIS AGREEMENT, THEN DO NOT CREATE A SERVICE ACCOUNT OR OTHERWISE USE THE PLATFORM OR OFFERINGS. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT, IN WHICH CASE THE TERMS "YOU" OR "CUSTOMER" SHALL REFER TO SUCH ENTITY. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT DOES NOT HAVE SUCH AUTHORITY, OR DOES NOT AGREE WITH THESE TERMS AND CONDITIONS, SUCH INDIVIDUAL MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE PLATFORM OR SERVICES.

1. Cloud Services

a. Randori Cloud Services

- Randori Cloud Services are "as a service" Randori offerings that Randori makes available via a network, such as software as a service, platform as a service, infrastructure as a service, or other network delivered services.
- Each Randori Cloud Service is described in a TD.
- Randori Cloud Services are designed to be available 24/7, subject to maintenance. Randori will provide advance notice of scheduled maintenance.

- Technical support and service level commitments, if any, are specified in an Attachment or TD.

b. Non-Randori Products

- Randori may offer Non-Randori Product, or an Randori Product may enable access to a Non-Randori Product.
- A TD will identify any applicable third party terms that govern Client's use of Non-Randori Products. Linking to or use of Non-Randori Products constitutes Client's agreement with such terms.
- Third-party terms and privacy practices govern use of a Non-Randori Cloud Service or other Service, including Content Client may provide, grant access to or input to.
- Randori will invoice Client for charges due and submit Client's order details to the third-party provider for the enablement and delivery of the Non-Randori Product.
- Randori is not a party to any third party agreement and is not responsible for Non-Randori Products.
- Access to ongoing Non-Randori Products may be discontinued at any time if the third party discontinues or Randori no longer makes available such Non-Randori Products.

c. Order Acceptance

- Client accepts the applicable Attachment or TD for Cloud Services by ordering, enrolling, using, or making a payment.
- Randori accepts Client's order by confirming the order or enabling access.

d. What Randori Provides

- Randori provides the facilities, personnel, equipment, software, and other resources necessary for Randori to provide Randori Cloud Services.
- Randori provides generally available user guides and documentation to support Client's use of Randori Cloud Services.

e. Enabling Software

- Enabling Software is software that Client downloads to Client systems that facilitates the use of a Cloud Service and will be identified in a TD.
- Enabling Software is not part of the Cloud Service and Client may use Enabling Software only in connection with use of the Cloud Service in accordance with any licensing terms specified in a TD.

- The licensing terms will specify applicable warranties, if any. **Otherwise, Enabling Software is provided as is, without warranties of any kind.**

f. What Client Provides

- Client will provide hardware, software and connectivity to access and use the Cloud Services, including any required Client-specific URL addresses and associated certificates.

g. Right to Use and Client Responsibilities

- Client's authorized users may access Cloud Services only to the extent of authorizations Client acquires.
- Client is responsible for the use of Cloud Services by any user who accesses the Cloud Services with Client's account credentials.

h. Acceptable Use Terms

- Cloud Services may not be used to undertake any activity or host Content that:
  (1) is unlawful, fraudulent, harmful, malicious, obscene, or offensive;
  (2) threatens or violates the rights of others;
  (3) disrupts or gains (or intends to disrupt or gain) unauthorized access to data, services, networks, or computing environments within or external to Randori;
  (4) sends unsolicited, abusive, or deceptive messages of any type; or
  (5) distributes any form of malware.
- Client may not use Cloud Services: i) for crypto-mining, unless otherwise agreed by Randori in writing; or ii) if failure or interruption of the Cloud Services could lead to death, serious bodily injury, or property or environmental damage.
- Client may not:
  (1) reverse engineer any portion of a Cloud Service;
  (2) assign or resell direct access to a Cloud Service to a third party outside Client's Enterprise; or
  (3) combine a Cloud Service with Client's value add to create a Client-branded solution that Client markets to its end user customers unless otherwise agreed by Randori in writing.

i. Preview Cloud Services

- Cloud Services or features of Cloud Services are considered "preview" when Randori makes such services or features available at no charge, with limited or pre-release functionality, or for a limited time to try available functionality. Examples of preview

Cloud Services include beta, trial, no-charge, or preview-designated Cloud Services.

- Any preview Cloud Service is excluded from available service level agreements and may not be supported.
- Randori may change or discontinue a preview Cloud Service at any time and without notice.
- Randori is not obligated to release preview Cloud Services or make an equivalent service generally available.

2. Content and Data Protection

- Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to Randori Cloud Services or information or data Client may provide, make available or grant access to, in connection with Randori providing other Services.

a. Content Client Provides

- Client grants the rights and permissions to Randori, its affiliates, and contractors of either, to use, provide, store, and otherwise process Content solely for the purpose of providing the Randori Cloud Services or other Services.
- Use of the Randori Cloud Services or other Services will not affect Client's ownership or license rights in Content.

b. Use of Content

- Randori, its affiliates, and contractors of either, will access and use the Content solely for the purpose of providing and managing the applicable Randori Cloud Service or other Services.
- Randori will treat Content as confidential by only disclosing to Randori employees and contractors to the extent necessary to provide the Randori Cloud Services or perform other Services.

c. Client Responsibilities

- Client is responsible for obtaining all necessary rights and permissions to permit processing of Content in the Randori Cloud Services or to provide other Services.
- Client will make disclosures and obtain consent Irequired by law before Client provides, authorizes access, or inputs individuals' information, including personal or other regulated data, for processing in the Randori Cloud Services or use by Randori in providing other Services.
- If any Content could be subject to governmental regulation or may require security measures beyond those specified by Randori for the Randori Cloud Services or to provide other Services, Client will not provide, allow access to, or input the Content for processing in

	the Randori Cloud Services or provide or allow access of Content to Randori to provide Services unless specifically permitted in the applicable TD or unless Randori has first agreed in writing to implement additional security and other measures. Client is responsible for adequate back-up of Content on Client managed systems prior to providing or allowing access to Randori to provide Services.
d. Data Protection	• Security at Randori principles, at https://www.randori.com/security/ apply for generally available standard Randori Cloud Services and other Services. • Specific security features and functions of a Randori Cloud Service or other Services will be described in the applicable Attachment or TD. • Client is responsible for selecting, ordering, enabling, and using available data protection features appropriate to support Client's use of the Cloud Services. • Client is responsible for assessing the suitability of the Cloud Services for the Content and Client's intended use or the use of Content with other Services Randori will provide. Client acknowledges that the use of Cloud Services or other Services meets Client's requirements and processing instructions required to comply with applicable laws.
e. Randori's Data Processing Addendum	• Randori's Data Processing Agreement (DPA) is found at https://www.randori.com/data-processing-agreement/. • The DPA specifies how Randori will process personal data contained in Content. • The DPA applies to personal data contained in Content, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); or ii) other data protection laws identified at https://www.randori.com/dpa-dpl apply. • Upon request by either party, Randori, Client or affiliates of either, will enter into additional agreements as required by law in the prescribed form for the protection of regulated personal data included in Content. The parties agree (and will ensure that their respective affiliates agree) that such additional agreements will be subject to the terms of the Agreement.
f. Removal of Content	• For Randori Cloud Services with self-managed features, Client can remove Content at any time. Otherwise, Randori will return or remove Content from Randori computing resources upon the

expiration or cancellation of the Randori Cloud Services, other Services, or earlier upon Client's request.

- Randori may charge for certain activities performed at Client's request (such as delivering Content in a specific format).
- Randori does not archive Content; however, some Content may remain in the Randori Cloud Services backup files until expiration of such files as governed by Randori's backup retention practices.

3. Changes and Withdrawal of Cloud Services

a. Randori Right to Change Cloud Services

- At any time and at Randori's discretion, Randori may change:
  (1) the Randori Cloud Services, including the corresponding published descriptions; and
  (2) the DSP and other published data security and privacy documentation for the Randori Cloud Services.
- The intent of any change to the above will be to:
  (1) make available additional features and functionality;
  (2) improve and clarify existing commitments; or
  (3) maintain alignment to current adopted operational and security standards or applicable laws.
  Changes will not degrade the security or data protection features or functionality of the Randori Cloud Services.
- Changes to the published descriptions, DSP, or published other documents as specified above, will be effective when published or on the specified effective date.
- Any changes that do not meet conditions specified above will only take effect, and Client accepts, upon:
  (1) a new order;
  (2) the term renewal date for the Cloud Services that automatically renew; or
  (3) notification from Randori of the change effective date for ongoing services that do not have a specified term.

b. Withdrawal of a Cloud Service

- Randori may withdraw Randori Cloud Services on 12 months' notice.
- Randori will continue to provide a withdrawn Randori Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another generally available Randori offering.
- Non-Randori Products may be discontinued at any time if the third party discontinues or Randori no longer makes available such services.

4. Warranties

a. Randori Warrants

- Randori warrants that it provides Randori Cloud Services or Randori Services using commercially reasonable care and skill and as described in the applicable TD.
- These warranties end when the Randori Cloud Services or other Services end.
- **These warranties are the exclusive warranties from Randori and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose.**

b. Warranty Limitations

- **Randori does not warrant uninterrupted or error-free operation of the Randori Cloud Services.**
- **Randori does not warrant it will correct all defects.**
- **While Randori endeavors to provide security measures to keep all data secure, Randori does not warrant Randori can prevent all third party disruptions or unauthorized third party access.**
- **Randori warranties will not apply if there has been misuse, modification, damage not caused by Randori, or failure to comply with written instructions provided by Randori.**
- **Randori makes preview Cloud Services or Non-Randori Products under the Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Client for Non-Randori Services.**

5. Charges, Taxes, and Payment

a. Charges

- Client's right to use a Randori Product or Non-Randori Product is contingent on Client paying applicable charges as specified in a TD or applicable agreement under which Client acquired the entitlements. Client is responsible to acquire additional entitlements in advance of any increase of its use.
- Client agrees to pay all applicable charges specified in a TD and charges for use in excess of authorizations.
- Charges are exclusive of any customs or other duty, tax, and similar levies imposed by any authority resulting from Client's acquisitions under the Agreement and will be invoiced in addition to such charges.
- Amounts are due upon receipt of the invoice from Randori and payable within 30 days of the invoice date to an account specified by Randori and late payment fees may apply.

- Prepaid Randori Products or Non-Randori Products must be used within the applicable period.
- Randori does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid, except as may be specified in an Agreement.
- If Randori commits to pricing for Cloud Services as specified in a TD, Randori will not change such pricing during the specified term. If there is not a specified commitment, then Randori may change pricing on thirty days' notice. A change applies on the invoice date or the first day of the charging period or new term on or after the effective date Randori specifies in the notice.

b. Withholding Taxes

- Client agrees to:
  (1) Pay any withholding tax directly to the appropriate government entity where required by law;
  (2) furnish a tax certificate evidencing such payment to Randori;
  (3) pay Randori only the net proceeds after tax; and
  (4) fully cooperate with Randori in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents.
- If Client imports, exports, transfers, accesses, or uses a Randori Product or Non-Randori Product across a border, Client agrees to be responsible for and pay authorities any custom, duty, tax, or similar levy assessed by the authorities. This excludes those taxes based on Randori's net income.
- Where taxes are based upon the location(s) receiving the benefit of the Cloud Services, Client has an ongoing obligation to notify Randori of such location(s) if different than Client's business address listed in the applicable Attachment or TD.

c. Invoicing

- Randori will invoice:
  (1) recurring charges at the beginning of the selected billing frequency term;
  (2) overage and usage charges in arrears; and
  (3) one-time charges upon Randori's acceptance of an order.

6. Liability and Intellectual Property Protection

a. Liability for Damages

- Randori's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim.

- **Randori will not be liable for special, incidental, exemplary, indirect or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.**
- These limitations apply collectively to Randori, its affiliates, contractors, and suppliers.

b. What Damages are Not Limited

- The following amounts are not subject to the above cap:
  (1) third party payments related to infringement claims described in subsection c below; and
  (2) damages that cannot be limited under applicable law.

c. Infringement Claims

- If a third party asserts a claim against Client that the Randori Product infringes a patent or copyright, Randori will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by Randori.
- To obtain Randori's defense against and payment of infringement claims, Client must promptly:
  (1) notify Randori in writing of the claim;
  (2) supply information requested by Randori; and
  (3) allow Randori to control, and reasonably cooperate in, the defense and settlement, including mitigation efforts.
- Randori's defense and payment obligations for infringement claims extend to claims of infringement based on open-source code that Randori selects and embeds in a Randori Product.

d. Claims Not Covered

- Randori has no responsibility for claims based on:
  (1) Non-Randori Products;
  (2) items not provided by Randori; or
  (3) any violation of law or third party rights caused by Content, or any Client materials, designs, or specifications.

7. Term and Termination

a. Term of a Cloud Service

- The term begins on the date Randori notifies Client that Client can access the Cloud Services.
- The ordering TD will specify whether the Cloud Services renew automatically, proceed on a continuous use basis, or terminate at the end of the term.
- For automatic renewal, unless Client provides written notice of non-renewal to Randori or the Randori Business Partner involved in the Cloud Services at least 30 days prior to the term expiration

date, the Cloud Services will automatically renew for the specified term.

- For continuous use, the Cloud Services will continue to be available on a month to month basis until Client provides 30 days written termination notice to Randori or the Randori Business Partner involved in the Cloud Services. The Cloud Services will remain available until the end of the calendar month after the 30-day period.

b. Suspension of a Randori Cloud Service

- Randori may suspend or limit, to the extent necessary, Client's use of a Randori Cloud Service if Randori reasonably determines there is a:
  (1) material breach of Client's obligations;
  (2) security breach;
  (3) violation of law; or
  (4) breach of the Acceptable Use Terms.
- Randori will provide notice prior to a suspension as commercially reasonable.
- If the cause of a suspension can reasonably be remedied, Randori will provide notice of the actions Client must take to reinstate the Randori Cloud Services. If Client fails to take such actions within a reasonable time, Randori may terminate the Randori Cloud Services.

c. Termination of Cloud Services

- Client may terminate the Randori Cloud Services on 30 days' notice:
  (1) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Randori Cloud Services;
  (2) if a change to the Randori Cloud Services causes Client to be noncompliant with applicable laws;
  (3) if Randori notifies Client of a change to the Randori Cloud Services that has a material adverse effect on Client's use of the Randori Cloud Services, provided that Randori will have 90 days to work with Client to minimize such effect.
- In the event of any such Client termination above or a similar termination of a Non-Randori Product, Randori will refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination.
- Client may terminate the Randori Cloud Services for material breach of Randori's obligations by giving notice and reasonable time to comply.

- If the Cloud Services are terminated for any other reason, Client will pay to Randori, on the date of termination, the total amounts due per the Agreement.
- Upon termination, Randori may assist Client in transitioning Content to an alternative technology for an additional charge and under separately agreed terms.

d. Termination of this CSA

- Either party may terminate:
  (1) this CSA without cause on at least 30 days' notice to the other after expiration or termination of its obligations under each Agreement; or
  (2) immediately for cause if the other is in material breach of the Agreement, provided the non-complying party is given notice and reasonable time to comply.
- Termination of this CSA does not terminate transactions in effect that are not affected by the cause of the material breach and provisions of the Agreement as they relate to such transactions remain in effect until fulfilled or otherwise terminated in accordance with their terms.
- Any terms, that by their nature extend beyond the CSA or Agreement termination, remain in effect until fulfilled and apply to successors and assignees
- Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Client's failure to pay, or Client providing inaccurate or fraudulent Client account or payment information to acquire Randori Products or Non-Randori Products, is a material breach.

8. Governing Laws and Geographic Scope

a. Applicable Laws

- Both parties agree to the application of the laws of the State of New York, United States, without regard to conflict of law principles.
- The rights and obligations of each party are valid only in the country of Client's business address.

b. Compliance with Laws

- Each party is also responsible for complying with:
  (1) laws and regulations applicable to its business and Content; and
  (2) import, export and economic sanction laws and regulations, including the defense trade control regime of the United States of America and any applicable jurisdictions that prohibit or restrict the import, export, re-export, or transfer of products, technology,

services or data, directly or indirectly, to or for certain countries, end uses or end users.
- Randori will not serve as Client's exporter or importer, except as required by data protection laws, for: i) any Content; or ii) use of any portion of a Cloud Service from a country outside Client's business address.

c. Enforcement and Other Rights

- If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect.
- Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract.
- The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

a. Randori's Role

- Randori is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary.
- Randori does not undertake to perform any of Client's regulatory obligations or assume any responsibility for Client's business or operations, and Client is responsible for its use of Randori Products and Non-Randori Products.
- Randori is acting as an information technology provider only.
- Randori's direction, suggested usage, or guidance or use of a Randori Product does not constitute medical, clinical, legal, accounting, or other licensed professional advice. Client should obtain their own expert advice.
- Each party is responsible for determining the assignment of its and its affiliates personnel, and their respective contractors, and for their direction, control, and compensation.

b. CSA Changes

- Since this CSA may apply to many future orders, Randori may change this CSA by providing Client at least 90 days' notice.
- CSA changes are not retroactive. They will only apply as of the effective date to:
  (1) new orders;
  (2) continuous Randori Products and Non-Randori Products that do not expire; and
  (3) renewals.
- For transactions with a defined renewable contract period stated in a TD, Client may request that Randori defer the change effective date until the end of the current contract period.

- Client accepts changes by placing new orders, continuing use after the change effective date, or allowing transactions to renew after receipt of the change notice.
- Except as provided in this section and the Changes and Withdrawal of Cloud Services section above, all other changes to the Agreement must be in writing accepted by both parties.

c. Business Conduct

- Randori maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud.
- Randori and its personnel comply with such policies and require contractors to have similar policies.

d. Business Contact and Account Usage Information

- Randori, its affiliates, and contractors of either require use of business contact information and certain account usage information. This information is not Content.
- Business contact information is used to communicate and manage business dealings with the Client. Examples of business contact information include name, business telephone, address, email, user ID, and tax registration information.
- Account usage information is required to enable, provide, manage, support, administer, and improve Randori Products. Examples of account usage information include digital information gathered using tracking technologies, such as cookies and web beacons during use of the Randori Cloud Services.
- The Randori Privacy Statement at https://www.randori.com/privacy-policy/ provides additional details with respect to Randori's collection, use, and handling of business contact and account usage information.
- When Client provides information to Randori and notice to, or consent by, the individuals is required for such processing, Client will notify individuals and obtain consent.

e. Randori Business Partners

- Randori Business Partners who use or make available Randori Products or Non-Randori Products are independent from Randori and unilaterally determine their prices and terms. Randori is not responsible for their actions, omissions, statements, or offerings.
- If Randori notifies Client their current Randori Business Partner will no longer resell a Randori Product, Client may select to acquire auto renewing or continuous use Cloud Services directly from Randori or from another authorized Randori Business Partner.

f. Assignment	• Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other except no consent is required if Randori assigns to International Business Machines ("IBM") or an IBM Company. • Randori may assign rights to receive payments. Randori will remain responsible to perform its obligations. • Assignments by Randori in conjunction with the sale of the portion of Randori's business that includes an Randori Product or Non-Randori Products is not restricted. • Randori may share this Agreement and related documents in conjunction with any assignment.
g. Enterprise Companies	• This CSA applies to Randori and Client (accepting this CSA) and their respective Enterprise companies that provide or acquire Randori Products or Non-Randori Products under this CSA. • The parties shall coordinate the activities of their own Enterprise companies under the CSA. • Enterprise companies include: (1) companies within the same country that Client or Randori control (by owning greater than 50% of the voting shares); and (2) any other entity that controls, is controlled by, or is under common control with Client or Randori and has signed a participation agreement.
h. Notices and Administration	• All notices under the Agreement must be in writing and sent to the business address specified for the Agreement, unless a party designates in writing a different address. • The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. • Any reproduction of the Agreement made by reliable means is considered an original. • The Agreement supersedes any course of dealing, discussions, or representations between the parties. • Where approval, acceptance, consent, access, cooperation, or similar action by either party is required, such action will not be unreasonably delayed or withheld.
i. Cause of Action	• No right or cause of action for any third party is created by the Agreement or any transaction under it. • Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose.

	• Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control.
j. Global Resources	• Randori may use personnel and resources in locations worldwide, including contractors, to support the delivery of Randori Products and Non-Randori Products. • Client's use of the Randori Products and Non-Randori Products may result in the transfer of Content, including personal data, across country borders. • A list of countries where Content may be transferred and processed is described the applicable TD or support documentation. • Randori is responsible for the obligations under the Agreement even if Randori uses a contractor and will have appropriate agreements in place to enable Randori to meet its obligations.
k. Use of Client Requested Third Party Services	• If Randori and Client agree to use a Client requested third party service to support the procurement or payment activities associated with an Agreement, Randori agrees to submit or receive applicable documents (such as invoices or similar contracting documents) using the third party service. • In the event: i) the third party service becomes unavailable for any reason; or ii) the third party provider modifies the service or terms of use in a manner Randori deems commercially unacceptable, the Client agrees to directly accept documents. • Client remains responsible to Randori for timely payments of invoices. • If there is a claim or proceeding against Randori related to Randori's proper use of Client's requested third party service, Client is responsible to reimburse Randori for reasonable defense costs and any amounts Randori is required to pay due to such claim or proceeding. This includes claims or proceedings due to the third party service provider's use, misuse, or disclosure of data or confidential information disclosed through the third party service or the third party's failure to comply with applicable data protection laws. Randori agrees to promptly notify Client in writing of any such claim or proceeding.

Service Description

Randori

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

The Randori Platform consists of the following offerings: Randori Recon, Randori Attack and Randori Attack – Targeted (individually or together are the Cloud Service).

1.1 Offerings

The Client may select from the following available offerings and order through their Randori sales representative accordingly.

1.1.1 Randori Recon

Randori Recon helps organizations continuously identify external facing assets that may be visible to attackers, both on-premises and in the cloud, and prioritizes potential exposures which pose the greatest risk. The cloud native SaaS solution is designed to help security teams focus on previously unknown and unmanaged exposure points.

Key capabilities:

- External Reconnaissance
- Shadow IT Identification
- M&A Risk Assessment
- Risk-Based Prioritization
- Integrations Marketplace
- Remediation Guidance

1.1.2 Additional Services – Randori Attack

Randori Attack is an add-on offering to Randori Recon that helps organizations validate their security program by testing their ability to detect, respond to, and remediate opportunistic attacks that are broadly applicable. Randori Attack builds on the detection capabilities of Randori Recon by adding authentic attacker automations such as vulnerability exploitation, credential stuffing, and post-exploitation actions-on-target (e.g. internal scanning, credential harvesting, data exfiltration). This offering allows security teams to practice realistic detection and response to common threats, and provides security executives the ability to assess the effectiveness of their security programs and procedures.

Key capabilities:

- Continuous testing for exploitable vulnerabilities and misconfigurations

- Vulnerability exploitation and post-exploitation pivoting for validation of detection and response to compromise
- Internal network reconnaissance for validation and testing of network configuration (e.g. segmentation)
- Testing of leaked credentials and default credentials
- Phishing campaigns to identify areas of risk and improve awareness
- Deployable “leave behind” to emulate insider threats
- Real-time reporting of attack activity

Client must have entitlement to Randori Recon as a prerequisite to acquiring Randori Attack.

1.1.3 Additional Services – Randori Attack Targeted

Randori Attack Targeted is an additional add-on offering to Randori Recon that extends the benefits of Randori Attack by adding objective-driven campaigns and after-action reporting. Organizations looking to extend their existing red team capabilities or those seeking an initial red team capability deploy Randori Attack Targeted to focus on specific objectives. Security executives and practitioners gain insights from objective-driven attack campaigns by experiencing end-to-end attack activity that often involve the compromise of multiple targets, crossing network segments, and advanced command and control techniques. By deploying attack techniques in a targeted objective-driven manner, organizations gain a realistic understanding of their ability to detect and respond to attackers targeting their critical assets.

Key capabilities

- Objective-Based Attacks

- Human Analysis of Secondary Data
- Custom Research and Development
- Remediation Guidance & Mitigation Strategies
- Monthly Findings Reports
- Attack Team Engagements

Client must have entitlement to Randori Recon as a prerequisite to acquiring Randori Attack Targeted.

2. Service Levels and Technical Support

The support and service level agreement located at https://www.randori.com/Platform-Support-SLA/ is incorporated herein by reference as updated from time to time. Trial Services do not include support or service level obligations.

3. Charges

3.1 Charge Metrics

The following charge metrics apply to this Cloud Service:

- Employee is a unique person employed in or otherwise paid by or acting on behalf of Client's Enterprise, whether or not given access to the Cloud Services.

4. Additional Terms

4.1 Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for Randori and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at Randori's then current rates and for other charges and liabilities determined as a result of such verification, as Randori specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

4.2 Trial Services

If Client's access to one or more of the offerings is for a trial or evaluation only ("Trial Services"), then the Client's access shall be limited to thirty days, or the term specified in writing by Randori. Client may not utilize the same Trial Services for more than one trial or evaluation term in any twelve month period, unless otherwise agreed to by Randori.

4.3 Ownership and Confidentiality of Security Vulnerability Information

Client acknowledges and agrees that the information and analysis regarding security vulnerabilities, potential security vulnerabilities and security issues created or generated by Randori in performance of the Cloud Service is confidential information of RANDORI, and that RANDORI owns all proprietary rights in such information ("RANDORI Confidential Information"). Client agrees to use the RANDORI Confidential Information solely for its lawful internal network security activities, and only to disclose the RANDORI Confidential Information to persons who have a need to know. Client is prohibited from publishing or distributing any portion of the RANDORI Confidential Information made available through the Cloud Service without the express written consent of RANDORI. Before disclosure to employees who have a need to know, Client will instruct such employees to treat the RANDORI Confidential Information substantially the same as described in the confidentiality provisions of this Agreement. With RANDORI's written consent, Client may disclose the RANDORI Confidential Information to consultants or contractors engaged by Client to assist Client with respect to security vulnerabilities, potential security vulnerabilities and/or security issues identified in such RANDORI Confidential Information provided such consultants or contractors are bound to confidentiality obligations and use restrictions at least as stringent as those

contained in this Agreement. Client shall be responsible for any breach of the confidentiality obligations by such consultants or contractors. If required to disclose information by law or court order, Client will, to the extent legally permitted, endeavor to give RANDORI prompt notice to allow RANDORI a reasonable opportunity to obtain a protective order at its sole cost and expense, and/or waive compliance with the applicable provisions of this Agreement. In the event that such protective order or other remedy is not obtained, or RANDORI waives compliance with the provisions of this Agreement, Client may furnish only that portion of the RANDORI Confidential Information which it is required to disclose.

RANDORI Confidential Information shall not include any information that (i) is or becomes generally available to the public through no fault of or action of the Client, (ii) is or becomes available to the Client on a non-confidential basis from a source, other than RANDORI, which, to Client's knowledge at the time of disclosure, is not bound by confidentiality obligations with respect thereto, (iii) was already in the possession of the Client on a non-confidential basis prior to its disclosure by RANDORI, or (iv) is or was developed independently by or on behalf of the Client without reference to the RANDORI Confidential Information.

4.4 Regulatory Compliance

The Cloud Service can be used to help Client meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the Cloud Service does not constitute legal, accounting, or other professional advice, and Client is cautioned to obtain its own legal, accounting, or other expert counsel. Client is solely responsible for ensuring that Client and Client's activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Cloud Service does not guarantee compliance with any law, regulation, standard or practice.

4.5 Authorization to Scan, Discover and Monitor Computer Systems

Randori Recon can be used to scan, discover, and monitor computer systems (which for purposes of this provision includes but is not limited to applications and IP addresses) used by Client or Client's Enterprise. Client is authorized to instruct Randori to deploy the Randori Recon on, with or against, the computer systems identified by the Client, or which are scanned, discovered, or monitored by Randori Recon as instructed by Client. Client has obtained or will obtain all necessary consents in connection with such deployment.

4.6 Authorization to Access Computer Systems

Randori Attack and Randori Attack Targeted (Attack Services) can be used to simulate cyber-security attacks on computer systems (which for purposes of this provision includes but is not limited to applications and IP addresses). Certain laws prohibit any unauthorized attempt to penetrate or access computer systems.

Client authorizes Randori to deploy Attack Services on, with or against the systems identified by Client within the platform, or otherwise in writing and acknowledge that such identification by Client constitutes authorized access to Client's computer systems.

For computer systems (which for purposes of this provision includes but is not limited to applications and IP addresses) owned by a third party that will be the subject of testing by Attack Services, Client agrees:

(1) that prior to Randori initiating testing on a third-party computer system, Client will obtain a signed consent from the owner of the third-party computer system authorizing Randori to test, penetrate or access that computer system via the Cloud Service, and to provide Randori with a copy of such authorization if needed; and
(2) to be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by the Cloud Service to the system owner.

5. Overriding Terms

5.1 Security Data

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: Randori will prepare and utilize de-identified and/or aggregate information collected from the Cloud Service (called "Security Data"). The Security Data will not identify the Client, or an individual except as provided in (d) below. Client herein additionally agrees that Randori may use and/or copy the Security Data only for the following purposes:

a. publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);
b. developing or enhancing products or services;
c. conducting research internally or with third parties; and
d. lawful sharing of confirmed third party perpetrator information.

5.2 Deviations from Randori Data Security and Privacy Principles

The security testing and vulnerability assessments as described in Section 9.1(2) of the Randori Data Security and Privacy Principles at https://www.randori.com/security are not performed before every production release but upon each significant change and in no event less than annually.
The vulnerability scanning as described in Section 9.1(4) of the Randori Data Security and Privacy Principles at https://www.randori.com/security/ is not fully automated but rather some vulnerability scans are performed manually.

5.3 Terms Applicable to the Cloud Services for Amazon Web Services (AWS) and Google Cloud Platform (GCP) and SpyCloud

The following prevails over anything to the contrary in the base Cloud Service terms between the parties:

The Cloud Service application layer (in whole or in part) and Client's data and content are hosted on a third-party cloud service platform not managed by Randori. The Cloud Service infrastructure, certain aspects of the Cloud Service platform, and related services, including: data center, servers, storage and network; application and data backup; perimeter security and threat detection; key and certificate management; and APIs for application deployment, monitoring and operation (collectively, the "Third Party Cloud Services") are hosted and managed by the third party provider. Accordingly, notwithstanding anything in this Agreement:

a. If AWS withdraws or terminates its services or Randori's or Client's access to such services, Randori may (i) provide Client access to a functionally-equivalent Randori-hosted Cloud Service offering; or (ii) terminate the Cloud Service immediately upon the effective date of such termination by AWS by providing notice of termination to Client.

b. Randori makes no warranties or conditions, express or implied, regarding the Third-Party Cloud Services or to the Cloud Service to the extent dependent on the Third-Party Cloud Services. The foregoing disclaimer does not apply to or limit compensation that may be payable under the Service Level Agreement section of this Service Description.

c. The Randori Data Security and Privacy Principles (DSP) and Data Processing Addendum (DPA) do not apply to the Third Party Cloud Services or to the Cloud Service solely to the extent dependent on or under the control of the Third-Party Cloud Services or the third party provider. With respect to such Third Party Cloud Services and the Cloud Service to the extent dependent on or under the control of the Third Party Cloud Services or the third party provider, the data protection and technical and operational security measures for the Cloud Service will be no less than those described in the AWS Customer Agreement and its referenced attachments available here: https://aws.amazon.com/agreement/, and the GCP Terms and its referenced attachments available here: https://cloud.google.com/terms/, and the SpyCloud security principles available here: https://spycloud.com/legal-and-privacy-center/governance-risk-and-compliance/.