KIKEN TECHNOLOGIES LLC

SECURITY TERMS AND CONDITIONS

FOR

DATA LOSS PREVENTION AND DATA SECURITY POSTURE MANAGEMENT PLATFORM

Effective Date: As defined in Section 1 (Definitions)

Last Updated: June 1, 2026

Version: 1.3

TERMS OF SERVICE

These Terms of Service (this **"Agreement"**) are entered into by and between Kiken Technologies LLC, an Indiana limited liability company (**"Kiken," "we," "us,"** or **"our"**), and the entity or individual identified in the applicable Order Form or account registration (**"Customer," "you,"** or **"your"**). By accessing or using the Kiken Platform, you agree to the terms of this Agreement and to be bound by this Agreement. If you are using this product and service or entering into this Agreement on behalf of a company or other legal entity, you represent that you have the authority both to purchase this product and to bind such entity to this Agreement.

If you do not agree to any or all of these terms, do not access or use the service, product, and Platform.

1. DEFINITIONS

"Affiliate" means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party, where "**control**" means ownership of more than fifty percent (50%) of the voting interests of the subject entity.

"Agent" means the Kiken software component deployed within the Customer Environment that facilitates Tracer Injection, DSPM Scanning, and phone-home telemetry functionality. Agents are licensed on a per-unit basis as specified in the applicable Order Form.

"Authorized Users" means the individuals authorized by Customer to access and use the Platform under Customer's subscription, as specified in the applicable Order Form.

"Configuration" means the settings, rules, policies, file-type selections, network parameters, and other specifications established by Customer within the Platform dashboard to define which files and data categories are subject to Tracer Injection and DSPM Scanning.

"Customer Data" means any data, files, documents, or information uploaded to, processed by, or monitored through the Platform by or on behalf of Customer, including without limitation any data into which Tracers are injected.

"Customer Environment" means Customer's network infrastructure, systems, endpoints, servers, cloud instances, and other computing resources to which the Platform is connected or deployed.

"DSPM Scanning" or "Scanning Services" means the Platform's data security posture management functionality, which scans the Customer Environment to identify, classify, and report on data assets, security posture, and configuration compliance in accordance with Customer's Configuration.

"Documentation" means the then-current user manuals, technical specifications, integration guides, API documentation, and other materials made available by Kiken describing the features, functionality, and requirements of the Platform, as may be updated by Kiken from time to time in accordance with Section 13.4.

"Effective Date" means, for an Enterprise Customer, the date of last signature on the signature page of this Agreement or the date specified in the applicable Order Form; and for a Customer subscribing through Kiken's standard online subscription process, the earlier of the date on which Customer first accepts this Agreement and the date on which Customer first accesses or uses the Platform.

"Enterprise Customer" means a Customer that has executed a negotiated Order Form containing terms individually negotiated between the parties, as distinguished from a Customer subscribing through Kiken's standard online subscription process.

"Order Form" means an ordering document or online subscription form executed by the parties or completed by Customer that references this Agreement and specifies the subscription tier, fees, term, number of Authorized Users, number of Agents, and other commercial terms.

"Platform" means the Kiken data loss prevention and data security posture management software-as-a-service platform, including all associated features, tools, APIs, dashboard interfaces, Tracer technology, DSPM Scanning functionality, and any updates, upgrades, or modifications thereto provided by Kiken during the Subscription Term.

"Professional Services" means any onboarding, implementation, configuration assistance, training, consulting, or other professional services provided by Kiken to Customer, as specified in an Order Form or statement of work.

"Subscription Term" means the period during which Customer is authorized to access and use the Platform, as specified in the applicable Order Form.

"Tracer" or "Tracer Technology" means Kiken's proprietary technology that embeds a persistent, non-displayed digital marker into files within the Customer Environment, which is designed to transmit location and status information ("**phone home**") to the Customer's Platform dashboard when the file is accessed, copied, moved, or exfiltrated from the Customer Environment.

"Tracer Injection" means the process by which the Platform embeds a Tracer into a file within the Customer Environment in accordance with Customer's Configuration.

2. SUBSCRIPTION AND ACCESS

2.1 Grant of Access

Subject to Customer's compliance with this Agreement and payment of all applicable fees, Kiken grants Customer a non-exclusive, non-transferable, non-sublicensable right to access

and use the service and Platform during the Subscription Term, solely for Customer's internal business purposes and in accordance with the Documentation and the applicable Order Form. The rights granted under this Agreement do not extend to, and no license is granted for, any use that violates this Agreement or applicable law.

2.2 Authorized Users and Agent Licensing

Customer may permit its Authorized Users within its organization to access the Platform, provided that Customer shall be responsible for all acts and omissions of its Authorized Users and for ensuring their compliance with this Agreement. Customer shall not permit any other person, entity, or third party to access the Platform using Customer's credentials. Customer's use of Agents is limited to the number of Agents specified in the applicable Order Form, including any later amendments and additions of additional Agents. To extend coverage to additional network segments, endpoints, or regions, Customer must disclose the additional Agents to Kiken and purchase additional Agent licensing through a new or amended Order Form.

2.3 Usage Restrictions

Customer shall not, and shall not permit any third party to: (a) sublicense, sell, lease, or otherwise transfer access to the Platform; (b) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code, algorithms, or underlying technology of the Platform, including without limitation any Tracer Technology; (c) modify, adapt, or create derivative works based on the Platform; (d) use the Platform in violation of any applicable law or regulation; (e) use the Platform to develop a competing product or service; (f) use the Platform for the purposes of product evaluation, benchmarking, competitive analysis, or other comparative analysis intended for publication or distribution outside Customer's organization without Kiken's prior written consent; (g) interfere with or disrupt the integrity or performance of the Platform; (h) attempt to gain unauthorized access to the Platform or its related systems or networks; or (i) remove, alter, or obscure any proprietary notices on the Platform.

3. DESCRIPTION OF SERVICES; TRACER TECHNOLOGY

3.1 Tracer Injection

The Platform provides data loss prevention capabilities through Kiken's proprietary Tracer Technology. When properly configured by Customer through the Platform dashboard, the Platform will scan the Customer Environment and inject Tracers into files that match Customer's Configuration parameters. Once injected, Tracers are designed to transmit status and location data to Customer's Platform dashboard.

3.2 Phone-Home Telemetry Functionality

Tracers are engineered to report their status and location to Customer's Platform dashboard when a file containing a Tracer is accessed, copied, transferred, or otherwise leaves the Customer Environment. The Platform is designed to maintain phone-home telemetry capability following the unauthorized removal of a file across a variety of network environments, including but not limited to virtual private networks (VPNs), virtual

machines (VMs), proxy servers, anonymizing networks, and other obfuscation or redirection techniques commonly employed by threat actors. The Tracer Technology is designed and provided solely to enable Customer to detect and investigate the unauthorized access to, movement of, or exfiltration of Customer's own data, and its use is subject to Section 5.

3.3 Limitations of Tracer Technology

Customer acknowledges and agrees that:

(a) No Tracer technology, and no data security service, including Kiken's, can guarantee phone-home telemetry functionality in one hundred percent (100%) of all circumstances or across all possible threat environments. While Tracers are designed to function in substantially all foreseeable exfiltration scenarios, there may be circumstances under which a Tracer fails to report, including without limitation situations involving:

(i) Advanced Persistent Threat ("**APT**") groups, including state-sponsored or nation-state threat actors, that may develop techniques currently unknown to Kiken to detect, remove, disable, neutralize, or otherwise defeat a Tracer;

(ii) Zero-day exploits or novel attack vectors that circumvent Tracer persistence mechanisms;

(iii) Air-gapped environments, Faraday-caged systems, or other network configurations that physically prevent outbound communication;

(iv) Complete destruction or corruption of the file containing the Tracer;

(v) Highly sophisticated counter-forensic or anti-analysis techniques that strip, overwrite, or neutralize embedded data within files; or

(vi) Jurisdictions or environments where internet access is restricted, monitored, or blocked by governmental authorities.

(b) The phone-home telemetry functionality of any given Tracer is dependent upon numerous factors outside of Kiken's control, including network availability, file integrity, and the threat actor's sophistication and methods.

(c) Kiken does not represent, warrant, or insure that Tracers will detect, report, or prevent any or all data exfiltration events or security incidents. The Platform is a risk-reduction tool and is not a guarantee against every possible data loss. It is one layer of a broader data loss prevention and remediation program.

3.4 Configuration-Dependent Functionality

The Platform's Tracer Injection and phone-home telemetry functionality is entirely dependent upon Customer's Configuration. Subject to and without limiting the limitation of liability set forth in this Agreement, Customer acknowledges and agrees that Kiken shall have no liability to Customer for any

data loss, for the failure to inject a Tracer into any file, or for any failure of an injected Tracer to report, including without limitation where such failure results directly or indirectly from:

(a) Customer's failure to properly configure the Platform dashboard, including without limitation the failure to select appropriate file types, directories, network segments, or data categories for Tracer Injection;

(b) Customer's failure to follow the Documentation or Kiken's published configuration guides and best practices;

(c) Changes to Customer's network architecture, file storage systems, security policies, or infrastructure that affect Platform operation and are not reflected in Customer's Configuration;

(d) Misconfiguration, improper deployment, or inadequate maintenance of the Customer Environment;

(e) Customer's disabling, overriding, or modification of any Platform feature or default setting; or

(f) Actions or omissions of Customer's employees, contractors, or Authorized Users that interfere with Platform operation.

For the avoidance of doubt: If Customer does not configure the Platform to inject Tracers into a particular file type, directory, network segment, or data category, and a file within that uncovered scope is subsequently accessed, copied, moved, or exfiltrated, Kiken shall bear no responsibility for the absence of a Tracer in that file or for any resulting loss or damage, regardless of the cause.

4. DATA SECURITY POSTURE MANAGEMENT (DSPM) SCANNING SERVICES

4.1 Scanning Functionality

The Platform provides DSPM Scanning capabilities that analyze the Customer Environment to identify, classify, and report on data assets, security posture, misconfigurations, access anomalies, and compliance status. Scanning operates in accordance with Customer's Configuration and the parameters established through the Platform dashboard.

4.2 Scope of Scanning

DSPM Scanning is limited to the systems, networks, endpoints, and data repositories that Customer has connected to and configured within the Platform. The Platform cannot scan systems or data stores that have not been integrated with the Platform or that are outside the scope of Customer's Configuration.

4.3 Scanning Limitations

Customer acknowledges that DSPM Scanning: (a) may not identify all security vulnerabilities, misconfigurations, or data exposures within the Customer Environment; (b) relies on Customer providing accurate and complete network topology, access credentials, and system integration information; (c) may produce false positives or false negatives; and (d) does not constitute a penetration test, security audit, or compliance certification. Customer is solely responsible for evaluating and acting upon the results of DSPM Scanning.

5. ACCEPTABLE USE; PROHIBITED CONDUCT; LAWFUL DEPLOYMENT

5.1 Permitted Purpose

The Platform, and in particular the Tracer Technology, is licensed solely to enable Customer to protect, monitor, and investigate the unauthorized access to, movement of, or exfiltration of Customer's own data within and from the Customer Environment, and to assess and improve the security posture of the Customer Environment. Customer shall use the Platform only for Customer's internal data-security and data-governance purposes with respect to data that Customer owns or that Customer is lawfully authorized to monitor, and only in compliance with this Agreement, the Documentation, and all applicable laws.

5.2 Authorization to Deploy

For every system, endpoint, network, repository, file, and category of data into or against which Customer directs Tracer Injection or DSPM Scanning, Customer represents, warrants, and covenants that Customer either owns such system or data or has obtained all authorizations, rights, and permissions necessary to deploy the Platform against it. Customer shall not deploy the Platform against any system, network, file, or data that Customer does not own or is not authorized to monitor.

5.3 Prohibited Conduct

Customer shall not, and shall not permit any Authorized User or any third party to, use the Platform or any Tracer:

(a) to track, locate, surveil, profile, or collect information about any natural person, except for (i) lawful monitoring of Customer's own workforce conducted with all notices and consents required by applicable law, and (ii) lawful investigation of an actual or reasonably suspected unauthorized exfiltration of Customer's own data;

(b) to embed a Tracer into any file or data that Customer intends to transmit, disclose, or make available to a third party for the purpose of tracking, surveilling, or collecting information about that third party or the recipients or custodians of such file, including without limitation opposing parties, opposing counsel, counterparties, competitors, journalists, or any other person; provided, however, that this Section 5.3(b) does not prohibit Customer from embedding a Tracer into a file containing Customer's own data that Customer shares with a vendor, contractor, service provider, or other recipient that Customer has engaged or authorized, where the Tracer is used for the purpose of protecting

that data and detecting its unauthorized access, movement, or exfiltration, and where Customer has, before or at the time of disclosure, informed the recipient that the file incorporates tracking technology and has obtained any consent required by applicable law;

(c) in connection with, or in any manner that would violate, any applicable law governing the interception of communications, electronic surveillance, wiretapping, computer fraud or unauthorized access, anti-stalking or anti-harassment, consumer protection, employee or workplace monitoring, or data protection, including without limitation the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, applicable state two-party-consent and anti-stalking statutes, the European Union General Data Protection Regulation ("**GDPR**"), the United Kingdom GDPR, and applicable United States state privacy laws;

(d) to surveil, target, intimidate, suppress, or facilitate harm to journalists, dissidents, activists, human-rights defenders, political opponents, or any other person on the basis of the exercise of fundamental rights, or in any manner that contributes to or facilitates a violation of human rights or the physical harm, persecution, or unlawful detention of any person;

(e) to stalk, harass, threaten, defame, or invade the privacy of any person;

(f) in violation of any applicable rule of professional responsibility, court rule, protective order, discovery obligation, or other legal process, or in any manner intended to circumvent, frustrate, or obstruct a legal or regulatory obligation; or

(g) for any unlawful, fraudulent, deceptive, or malicious purpose, or in any manner not expressly authorized by this Agreement.

5.4 Notices, Consents, and Lawful Basis

Customer is solely responsible for determining whether, and for ensuring that, its deployment and use of the Platform is lawful in each applicable jurisdiction, and for obtaining and maintaining all rights, authorizations, lawful bases, notices, and consents required for the deployment of Tracers, for DSPM Scanning, for the monitoring of file access and movement, and for the collection and transmission of any information, including personal data of individuals both within and outside the Customer Environment, generated by Tracer phone-home telemetry events. Where required by applicable law, Customer shall provide all notices to, and obtain all consents from, individuals whose data may be processed through the Platform, and shall conduct any data protection impact assessment, legitimate-interests balancing test, or similar assessment required before deployment.

5.5 No Authorization of Misuse; Customer Acts as Principal

Kiken does not authorize, condone, encourage, or endorse any use of the Platform that violates this Agreement or any applicable law. Any such use is outside the scope of the license granted under this Agreement, constitutes a material breach of this Agreement, and is undertaken by Customer solely on its own behalf and in its own name, and not as an agent, representative, joint venturer, or partner of Kiken. Kiken designs, licenses, and

provides the Platform as a defensive data-security tool, and disclaims any intent that the Platform be used for unlawful surveillance or for any conduct prohibited by Section 5.3. As between the parties, Customer is solely the controller of, and the decision-maker with respect to, the configuration, targets, scope, timing, and purposes of its deployment of the Platform, and Kiken has no role in and no responsibility for those decisions.

5.6 No Duty to Monitor; Right to Investigate and Suspend

Kiken does not, in the ordinary course, monitor Customer's specific Configuration or the content of Tracer reports, and has no obligation to review, police, or pre-approve Customer's use of the Platform. Notwithstanding the foregoing, Kiken reserves the right, but assumes no obligation, to investigate any suspected violation of this Section 5 or of applicable law, to require information from Customer regarding its use of the Platform, to cooperate with law enforcement and governmental authorities and to respond to valid legal process, and to suspend or terminate Customer's access in accordance with Section 17.

5.7 Sensitive Deployments

Kiken may, in its discretion, decline to provide, condition the provision of, or discontinue the Platform for any deployment that Kiken reasonably believes presents a heightened risk of the conduct prohibited by Section 5.3, including deployments by or for governmental, law-enforcement, military, or intelligence end users. Upon Kiken's request, Customer shall provide an end-use and end-user certification in a form reasonably specified by Kiken.

6. CUSTOMER RESPONSIBILITIES; CONFIGURATION AND DEPLOYMENT

6.1 Configuration Obligations

Customer is solely responsible for: (a) the initial and ongoing configuration of the Platform, including the selection of file types, data categories, directories, network segments, and policies for Tracer Injection and DSPM Scanning; (b) ensuring that the Configuration accurately reflects Customer's data protection objectives and environment; (c) reviewing and updating the Configuration as Customer's environment, infrastructure, or data protection requirements change; and (d) testing and validating that the Configuration produces the intended results within the Customer Environment.

6.2 Environment Requirements

Customer shall ensure that the Customer Environment meets the minimum technical requirements specified in the Documentation, including but not limited to operating system versions, network configurations, firewall rules, outbound connectivity requirements, and endpoint agent deployment specifications. Customer acknowledges that failure to meet these requirements may materially impair Platform functionality and intended protections.

6.3 Security Practices

Customer acknowledges that the Platform is one component of a comprehensive security strategy and is not a substitute for prudent security practices. Customer shall maintain reasonable security measures within the Customer Environment, including but not limited

to access controls, network segmentation, endpoint protection, patch management, incident response planning, employee security awareness training, and regular security assessments. Customer understands that the Platform is not an insurance product and does not provide insurance coverage for data loss or infiltration, and that Customer, at its option, will select and maintain its own data loss, data infiltration, and cyber insurance coverage appropriate to Customer's risk profile and as determined by its internal risk management personnel. Kiken offers no opinion or advice to Customer as to the amount or type of any related insurance coverage.

6.4 Cooperation

Customer shall provide Kiken with reasonable cooperation, access, and information necessary for Kiken to deliver the Platform and any Professional Services. Customer shall promptly notify Kiken of any material changes to the Customer Environment that may affect Platform operation.

6.5 Compliance with Laws

Customer is solely responsible for ensuring that its use of the Platform, including the deployment of Tracers and DSPM Scanning within the Customer Environment, complies with all applicable federal, state, administrative, and local laws, regulations, and industry standards, including without limitation data protection, privacy, employment, and electronic surveillance laws applicable to Customer's jurisdiction and industry. Customer does and shall forever hold Kiken harmless, and shall defend Kiken, from any and all claims made by any party in reference to the use of the Platform for alleged violations of any law or standard, in accordance with Section 16.

7. SHARED RESPONSIBILITY MODEL

The parties acknowledge and agree that, notwithstanding the limitation and exclusion of liability set forth in this Agreement and Customer's continuing security responsibilities, the allocation of security responsibilities between Kiken and Customer is set forth in Exhibit C (Shared Responsibility Matrix), which is incorporated herein by reference. In general:

Kiken shall provide: the security, availability, and integrity of the Platform infrastructure; the maintenance and updating of the Tracer Technology and the DSPM Scanning engine; the application of security patches to Platform components; secure API endpoints; the encryption of Customer Data in transit and at rest within the Platform; and the maintenance of the Platform's SOC 2 Type II compliance (or equivalent).

Customer is responsible for: the configuration of the Platform; the complete and up-to-date number of Agents; the security of the Customer Environment; the management of Authorized User accounts and credentials; the accuracy and completeness of system integrations; compliance with applicable laws regarding the deployment of Tracers and monitoring within Customer's systems; and all decisions made in reliance upon Platform outputs, reports, and alerts.

8. PROFESSIONAL SERVICES

8.1 Scope

Kiken may provide Professional Services to Customer as specified in an Order Form or a mutually executed statement of work ("**SOW**"). Each SOW shall describe the scope, deliverables, timeline, and fees for such Professional Services and shall be governed by this Agreement.

8.2 Professional Services Warranty

Notwithstanding the limitation and exclusion of Kiken's liability set forth in this Agreement, Kiken's Professional Services will be performed as stated herein and consistent with reasonable industry standards. Customer must notify Kiken in writing of any alleged failure by Kiken within thirty (30) days of the performance of the applicable Professional Services.

8.3 Sole Remedy for Professional Services

Customer's sole and exclusive remedy, and Kiken's sole and entire liability, for any claimed deficiency in Professional Services under Section 8.2 shall be, at Kiken's option: (a) re-performance of the applicable Professional Services at no additional charge; or (b) if Kiken is unable to re-perform in a manner that substantially meets the applicable description within thirty (30) days of written notice, a refund of the fees paid for the deficient Professional Services and the affected period. This remedy is limited to the period of the deficiency and shall not be construed as covering the entire scope of the engagement or all previous fees paid. **This Section 8.3 describes the sole and exclusive remedy of Customer and the entire liability of Kiken with respect to any claim arising from or relating to Professional Services.**

8.4 Customer Dependencies

Kiken's obligation to perform Professional Services is contingent upon Customer's payment of all fees due to Kiken and Customer's timely provision of access, information, resources, and cooperation as reasonably required. Delays caused by Customer shall not constitute a failure by Kiken, and Kiken shall be entitled to adjust timelines accordingly.

9. INTELLECTUAL PROPERTY

9.1 Kiken IP

Kiken and its licensors retain all right, title, and interest in and to the Platform, including all Tracer Technology, scanning algorithms, software, documentation, trademarks, patents (including any patent-pending technology), copyrights, trade secrets, and all other intellectual property rights therein. This Agreement does not convey to Customer any ownership interest in or to the Platform, but only a limited right of access and use as expressly set forth herein, for the period and fees set forth in the Order Form.

9.2 Customer Data

As between the parties, Customer retains all right, title, and interest in and to Customer Data. Customer grants Kiken a non-exclusive, worldwide, royalty-free license to access,

process, and use Customer Data solely to the extent necessary to provide the Platform and related services during the Subscription Term.

9.3 Aggregated Data

Kiken may collect, aggregate, and anonymize data derived from Customer's use of the Platform ("**Aggregated Data**") for purposes of improving the Platform, developing threat intelligence, generating benchmarks, and for other lawful business purposes, provided that such Aggregated Data does not identify Customer or any individual. Kiken owns all right, title, and interest in Aggregated Data.

9.4 Feedback

If Customer provides Kiken with any suggestions, enhancement requests, recommendations, or other feedback regarding the Platform ("**Feedback**"), Customer hereby assigns to Kiken all right, title, and interest in such Feedback, and Kiken shall be free to use, incorporate, and commercialize any Feedback without restriction or obligation.

10. FEES AND PAYMENT

10.1 Fees

Customer shall pay all fees specified in the applicable Order Form. Unless otherwise stated in the Order Form, all fees are quoted in U.S. dollars and are due net thirty (30) days from the invoice date. **All fees owed pursuant to an Order Form are non-cancellable and non-refundable for the applicable Subscription Term.** Customer's obligation to pay fees is unconditional and is not subject to any right of set-off, counterclaim, or deduction. Service commences upon full payment of the fees set forth in the applicable Order Form.

10.2 Late Payment

Any amounts not paid when due shall accrue interest at the lesser of one and one-half percent (1.5%) per month or the maximum rate permitted by applicable law. Kiken reserves the right to recover all costs of collection, including court costs and attorneys' fees, incurred in connection with any unpaid fees.

10.3 Suspension for Non-Payment and Credit Risk

Kiken may suspend Customer's access to the Platform: (a) upon fifteen (15) days' written notice of non-payment if payment is not received within such notice period; or (b) immediately if Kiken has reasonable grounds to believe that Customer will not make timely payment, including but not limited to Customer's insolvency, material deterioration of Customer's creditworthiness, or a pattern of late payments. Suspension under this Section shall not relieve Customer of its payment obligations.

10.4 Taxes

All state and local taxes applicable in each jurisdiction will be added to Customer invoicing. Customer is responsible for all sales, sales and use, value-added, withholding, and other

taxes imposed on the transactions contemplated by this Agreement, excluding taxes based on Kiken's net income.

10.5 Disputed Invoices

If Customer disputes any invoice in good faith, Customer shall: (a) provide written notice to Kiken within ten (10) business days of receipt of the disputed invoice, specifying in reasonable detail the nature and basis of the dispute; (b) pay all undisputed amounts by the original due date; and (c) cooperate in good faith with Kiken to resolve the dispute within thirty (30) days of written notice. If the parties are unable to resolve the dispute within such thirty (30) day period, either party may pursue the dispute resolution procedures set forth in Section 22. Failure to provide timely written notice of a dispute shall constitute a waiver of Customer's right to dispute such invoice.

10.6 Agent-Based Licensing

Customer's use of the Platform is licensed on a per-Agent basis. The number of Agents licensed to Customer is specified in the applicable Order Form. Customer may not deploy Agents in excess of the licensed quantity without executing a new or amended Order Form. If Customer requires coverage for additional network segments, regions, or endpoints beyond those covered by its existing Agent allocation, Customer must purchase additional Agents at Kiken's then-current pricing. Customer will at all times be responsible for the fees for all Agents utilizing the Platform.

11. CONFIDENTIALITY

11.1 Confidential Information

Each party ("**Disclosing Party**") may disclose to the other party ("**Receiving Party**") certain non-public information that is designated as confidential or that a reasonable person would understand to be confidential given the nature of the information and the circumstances of disclosure ("**Confidential Information**"). Kiken's Confidential Information includes the Platform, the Tracer Technology, pricing, security architecture, and all proprietary methodologies. Customer's Confidential Information includes Customer Data and Configuration details.

11.2 Obligations

The Receiving Party shall: (a) hold Confidential Information in strict confidence using at least the same degree of care it uses for its own confidential information, but no less than reasonable care; (b) not disclose Confidential Information to any third party except as expressly permitted herein or with the Disclosing Party's prior written consent; and (c) use Confidential Information solely for the purposes of this Agreement.

11.3 Exceptions

Confidential Information does not include information that: (a) is or becomes publicly available without breach of this Agreement; (b) was known to the Receiving Party prior to disclosure without restriction; (c) is independently developed by the Receiving Party without use of Confidential Information; or (d) is rightfully received from a third party

without restriction. A Receiving Party may disclose Confidential Information to the extent required by law or court order, provided it gives the Disclosing Party prompt written notice and reasonable cooperation to seek a protective order.

12. DATA PROCESSING AND PRIVACY

To the extent Kiken processes personal data on behalf of Customer, the parties' respective obligations regarding such processing shall be governed by the Data Processing Addendum attached hereto as Exhibit B, which is incorporated by reference. Customer represents and warrants that it has obtained and will maintain all rights, authorizations, lawful bases, notices, and consents required under applicable data protection and privacy laws for the deployment of Tracers within, and the scanning of, the Customer Environment, including without limitation the monitoring of file access and movement and the collection and transmission to the Platform of all information generated by Tracer phone-home telemetry events, and including the personal data of individuals who are not within the Customer Environment and who access, hold, or transmit files containing Tracers. Customer acknowledges that, as between the parties, Customer is the controller and the sole determiner of the purposes and means of such processing, and that Kiken processes such data solely as a processor on Customer's documented instructions and in reliance on Customer's lawful basis. Customer shall defend and hold Kiken harmless, in accordance with Section 16, from any and all claims arising from Customer's failure to obtain or maintain any required rights, authorizations, lawful bases, notices, or consents, or from Customer's unlawful deployment or use of the Platform.

13. LIMITED WARRANTY

13.1 Platform Performance Warranty

Kiken warrants that, during the Subscription Term, the Platform will perform substantially in accordance with the Documentation when used in compliance with this Agreement and the Documentation. This warranty applies only when the Platform is properly configured by Customer in accordance with the Documentation and Kiken's published configuration guides.

13.2 Sole Remedy for Platform Warranty

Customer's sole and exclusive remedy, and Kiken's sole and entire liability, for any breach of the warranty set forth in Section 13.1 shall be, at Kiken's option: (a) commercially reasonable efforts to correct the non-conformity; or (b) if Kiken is unable to correct such non-conformity within sixty (60) days following written notice from Customer, termination of the affected subscription and a pro rata refund of prepaid fees for the unused portion of the Subscription Term. **This Section 13.2 describes the sole and exclusive remedy of Customer and the entire liability of Kiken with respect to any claim arising from or relating to the Platform's performance or functionality.**

13.3 Warranty Conditions

The warranty in Section 13.1 shall not apply to the extent any non-conformity results from: (a) use of the Platform other than in accordance with the Documentation; (b) modifications

to the Platform not authorized by Kiken; (c) combination of the Platform with third-party software, hardware, or services not approved by Kiken; (d) Customer's failure to implement updates or patches provided by Kiken; or (e) issues arising from the Customer Environment, including misconfigurations, infrastructure failures, or network issues.

13.4 Documentation Updates

Kiken may update the Documentation from time to time in its sole discretion to reflect changes in the Platform's features, functionality, configuration requirements, or best practices, provided that such updates shall not materially diminish the core functionality of the Platform during the then-current Subscription Term. Updated Documentation shall be made available through Kiken's standard documentation channels.

14. DISCLAIMER OF WARRANTIES

EXCEPT FOR THE EXPRESS LIMITED WARRANTIES SET FORTH IN SECTIONS 13.1 AND 8.2, THE PLATFORM, ALL PROFESSIONAL SERVICES, AND ALL RELATED SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." KIKEN HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

WITHOUT LIMITING THE FOREGOING, KIKEN MAKES NO WARRANTY OR REPRESENTATION THAT:

(A) THE PLATFORM WILL DETECT, PREVENT, REPORT, OR MITIGATE ALL DATA LOSS EVENTS, UNAUTHORIZED ACCESS, SECURITY BREACHES, EXFILTRATION ATTEMPTS, OR OTHER SECURITY INCIDENTS;

(B) TRACERS WILL SUCCESSFULLY PHONE HOME OR REPORT THEIR STATUS IN EACH AND EVERY CASE, UNDER ALL CONDITIONS, OR ACROSS ALL THREAT ENVIRONMENTS;

(C) THE PLATFORM WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE;

(D) THE PLATFORM WILL IDENTIFY ALL VULNERABILITIES, MISCONFIGURATIONS, OR SECURITY EXPOSURES WITHIN THE CUSTOMER ENVIRONMENT;

(E) THE PLATFORM WILL OPERATE EFFECTIVELY AGAINST ADVANCED PERSISTENT THREATS (APTS), STATE-SPONSORED THREAT ACTORS, ZERO-DAY EXPLOITS, OR NOVEL ATTACK VECTORS CURRENTLY UNKNOWN TO KIKEN; OR

(F) THE RESULTS OBTAINED FROM USE OF THE PLATFORM WILL BE ACCURATE, RELIABLE, OR COMPLETE.

CUSTOMER ACKNOWLEDGES THAT NO DATA LOSS PREVENTION, DATA SECURITY POSTURE MANAGEMENT, OR CYBERSECURITY SOLUTION CAN GUARANTEE COMPLETE PROTECTION AGAINST ALL THREATS. THE PLATFORM IS A RISK-REDUCTION TOOL DESIGNED TO SUBSTANTIALLY REDUCE THE LIKELIHOOD OF UNDETECTED DATA LOSS AND TO IMPROVE CUSTOMER'S SECURITY POSTURE. IT IS NOT INSURANCE, AND IT IS NOT A GUARANTEE AGAINST DATA LOSS OR SECURITY INCIDENTS. CUSTOMER IS SOLELY RESPONSIBLE FOR MAINTAINING COMPREHENSIVE SECURITY PRACTICES, POLICIES, PROCEDURES, AND INSURANCE COVERAGE APPROPRIATE TO CUSTOMER'S RISK AND RISK MANAGEMENT PROFILE.

15. LIMITATION OF LIABILITY

15.1 Exclusion of Consequential Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR:

(A) LOSS OF DATA, INCLUDING CUSTOMER DATA THAT WAS EXFILTRATED, STOLEN, DESTROYED, CORRUPTED, OR OTHERWISE COMPROMISED;

(B) LOSS OF REVENUE, PROFITS, GOODWILL, OR BUSINESS OPPORTUNITIES;

(C) BUSINESS INTERRUPTION OR LOSS OF USE;

(D) THE COST OF DATA BREACH NOTIFICATION, CREDIT MONITORING, FORENSIC INVESTIGATION, OR REMEDIATION;

(E) REGULATORY FINES, PENALTIES, OR ASSESSMENTS IMPOSED BY ANY GOVERNMENTAL AUTHORITY;

(F) THIRD-PARTY CLAIMS ARISING FROM OR RELATED TO A SECURITY INCIDENT, DATA BREACH, OR DATA LOSS EVENT;

(G) REPUTATIONAL HARM OR DAMAGE;

(H) THE FAILURE OF ANY TRACER TO PHONE HOME, REPORT, OR OTHERWISE FUNCTION AS INTENDED; OR

(I) THE FAILURE OF DSPM SCANNING TO IDENTIFY ANY VULNERABILITY, MISCONFIGURATION, OR EXPOSURE;

IN EACH CASE WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER LEGAL

THEORY, AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND REGARDLESS OF THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY PROVIDED HEREIN. Nothing in this Section 15.1 limits a party's indemnification obligations under Section 16 with respect to amounts payable to a third party (including damages, settlements, fines, penalties, and reasonable attorneys' fees), even where such amounts are in the nature of indirect or consequential damages of the third party.

15.2 Cap on Direct Damages

SUBJECT TO SECTIONS 15.3 AND 15.4, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AGGREGATE LIABILITY OF EITHER PARTY UNDER THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES ACTUALLY PAID OR PAYABLE BY CUSTOMER TO KIKEN DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM (THE "GENERAL CAP").

15.3 Increased Cap

Notwithstanding Section 15.2, the aggregate liability of either party for breach of Section 11 (Confidentiality) shall not exceed two times (2x) the General Cap.

15.4 Exclusions from the Cap

The General Cap and the Increased Cap do not apply to, and the following are not subject to any cap on liability under this Agreement: (a) Customer's obligation to pay fees; (b) either party's liability for fraud, willful misconduct, or gross negligence; (c) Kiken's indemnification obligations under Section 16.1 (IP Indemnification); (d) Customer's indemnification obligations under Section 16.3 (Customer Indemnification); (e) Customer's breach of Section 2.3 (Usage Restrictions), Section 5 (Acceptable Use; Prohibited Conduct; Lawful Deployment), or Section 9 (Intellectual Property); and (f) Customer's breach of Section 12 (Data Processing and Privacy), and any liability arising from Customer's unlawful deployment or use of the Platform.

15.5 Basis of the Bargain; Mutual Acknowledgment

The parties specifically acknowledge that the limitations and exclusions set forth in this Section 15 are reflected in Kiken's pricing and form an essential basis of the bargain between the parties. These limitations reflect a reasonable allocation of risk between the parties and shall apply notwithstanding any failure of the essential purpose of any limited remedy. Both parties acknowledge that they have freely negotiated these limitations, that the fees payable hereunder reflect such allocation, and that absent these limitations, the fees for the Platform would be substantially higher. Each party has had the opportunity to consult with legal counsel regarding these provisions.

16. INDEMNIFICATION

16.1 Kiken Indemnification (IP)

Kiken shall defend, indemnify, and hold harmless Customer and its officers, directors, employees, and agents from and against any third-party claim alleging that Customer's authorized use of the Platform infringes or misappropriates such third party's intellectual property rights ("**IP Claim**"), and shall pay any damages finally awarded or settlement amounts agreed to by Kiken. If an IP Claim is made or appears likely, Kiken may, at its sole option: (a) procure the right for Customer to continue using the Platform; (b) modify the Platform to make it non-infringing without materially diminishing functionality; or (c) if neither (a) nor (b) is commercially reasonable, terminate the affected subscription and refund any prepaid fees for the unused Subscription Term.

This Section 16.1 describes the sole and exclusive remedy of Customer and the entire liability of Kiken with respect to any IP Claim or any claim of infringement or misappropriation of intellectual property rights.

16.2 IP Indemnification Exclusions

Kiken's indemnification obligation under Section 16.1 shall not apply to the extent an IP Claim arises from: (a) modifications to the Platform made by anyone other than Kiken; (b) Customer's combination of the Platform with third-party products, services, or data not contemplated by the Documentation; (c) Customer's use of the Platform in violation of this Agreement; (d) Customer's continued use of a version of the Platform after Kiken has provided an updated, non-infringing version; or (e) any unauthorized use of the Platform or any use during a period of non-payment.

16.3 Customer Indemnification

Customer shall defend, indemnify, and hold harmless Kiken and its Affiliates, officers, directors, employees, and agents from and against any third-party claim, and any governmental or regulatory investigation, action, fine, or penalty, arising from or related to: (a) Customer Data, including any claim that Customer Data infringes or misappropriates any third party's rights; (b) Customer's use of the Platform in violation of this Agreement or applicable law; (c) Customer's configuration, deployment, or use of the Tracer Technology or DSPM Scanning, including any claim that such configuration, deployment, or use violated the privacy, publicity, data protection, or other legal rights of any person, constituted unlawful interception, surveillance, monitoring, stalking, or harassment, or contributed to harm to any person; (d) any violation by Customer of Section 5 (Acceptable Use; Prohibited Conduct; Lawful Deployment); (e) Customer's failure to obtain or maintain any rights, authorizations, lawful bases, notices, or consents required under Section 12; or (f) Customer's failure to maintain adequate security practices within the Customer Environment.

16.4 Indemnification Procedure

The indemnified party shall: (a) promptly notify the indemnifying party in writing of any claim (provided that failure to provide prompt notice shall not relieve the indemnifying party of its obligations except to the extent materially prejudiced); (b) grant the indemnifying party sole control of the defense and settlement of the claim; and (c) provide reasonable cooperation at the indemnifying party's expense. The indemnifying party shall

not settle any claim in a manner that imposes liability or obligations on the indemnified party without its prior written consent, not to be unreasonably withheld.

17. TERM AND TERMINATION

17.1 Term

This Agreement commences on the Effective Date and continues until all subscriptions hereunder have expired or been terminated. Each Subscription Term shall be as specified in the applicable Order Form and shall automatically renew for successive periods equal to the initial Subscription Term unless either party provides written notice of non-renewal at least sixty (60) days prior to the expiration of the then-current term.

17.2 Termination for Cause

Either party may terminate this Agreement: (a) upon thirty (30) days' written notice if the other party materially breaches this Agreement and fails to cure such breach within the notice period; or (b) immediately upon written notice if the other party becomes insolvent, makes an assignment for the benefit of creditors, or becomes the subject of any bankruptcy or similar proceeding.

17.3 Suspension or Termination for Misuse or Unlawful Use

Notwithstanding Section 17.2, Kiken may suspend Customer's access to the Platform immediately and without a cure period, or terminate this Agreement immediately upon written notice, if Kiken reasonably believes that Customer has violated Section 5 (Acceptable Use; Prohibited Conduct; Lawful Deployment) or has used the Platform in violation of applicable law, or if Kiken reasonably believes that continued provision of the Platform may expose Kiken to legal liability, may facilitate harm to any person, or may violate applicable law. Kiken will use commercially reasonable efforts to provide notice where practicable. Suspension or termination under this Section does not relieve Customer of its payment obligations and is without prejudice to Kiken's other rights and remedies.

17.4 Effect of Termination

Upon termination or expiration: (a) all rights granted hereunder shall immediately cease; (b) Customer shall cease all use of the Platform; (c) each party shall return or destroy the other party's Confidential Information; and (d) Kiken shall make Customer Data available for export for thirty (30) days following termination, after which Kiken may delete Customer Data. Sections 1, 2.3, 5, 6, 9, 10, 11, 12, 14, 15, 16, 20, and 22 shall survive any termination or expiration of this Agreement, together with any accrued rights to payment and any other provisions that by their nature are intended to survive.

18. SERVICE LEVEL AGREEMENT

Kiken shall use commercially reasonable efforts to maintain Platform availability in accordance with the Service Level Agreement attached hereto as Exhibit A. **Service credits issued under the SLA shall constitute Customer's sole and exclusive**

remedy, and Kiken's sole and entire liability, for any failure to meet the availability commitments specified therein.

19. *FORCE MAJEURE*

Neither party shall be liable for any failure or delay in performing its obligations under this Agreement (other than payment obligations) to the extent such failure or delay results from circumstances beyond such party's reasonable control, including but not limited to acts of God, natural disasters, war, terrorism, riots, embargoes, acts of governmental authorities, epidemics or pandemics, power failures, telecommunications failures, internet service disruptions, denial-of-service attacks, cyberattacks against the Platform infrastructure by third parties, and service disruptions involving hardware, software, or power systems not within such party's possession or reasonable control, including disruptions affecting third-party cloud hosting providers, content delivery networks, and infrastructure-as-a-service platforms upon which the Platform relies, or changes in applicable law or regulation. The affected party shall provide prompt notice and use commercially reasonable efforts to mitigate the impact of the force majeure event.

20. EXPORT COMPLIANCE AND END-USE RESTRICTIONS

20.1 Trade Controls

Customer acknowledges that the Platform may be subject to the export control, economic sanctions, customs, import, and anti-boycott laws, regulations, and orders of the United States and other jurisdictions having jurisdiction over the parties ("**Trade Controls**"). Customer shall ensure that the Platform is not directly or indirectly exported, re-exported, provided, or transferred (a) without any requisite authorizations, approvals, or licenses required under applicable Trade Controls, or (b) to any jurisdiction subject to a comprehensive embargo by any applicable Trade Controls, or to any person or entity listed on, or that is fifty percent (50%) or more owned or otherwise controlled by persons listed on, any applicable restricted or prohibited persons list, including the U.S. Entity List and the Specially Designated Nationals and Blocked Persons List (collectively, "**Restricted Persons**"). Customer represents and warrants that it is not located in an embargoed jurisdiction, is not a Restricted Person, and is not owned or controlled by any Restricted Person.

20.2 Prohibited End Uses

Customer shall not use, and shall not permit the Platform to be used, (a) for any military, nuclear, chemical, or biological weapons application or for the proliferation of such weapons; (b) for any unlawful surveillance, or in any manner that contributes to or facilitates a violation of human rights, including the conduct prohibited by Section 5.3(d); or (c) for any other end use or by any end user prohibited by applicable Trade Controls. Upon Kiken's request, Customer will complete and provide an end-use certificate in the form reasonably requested by Kiken. Kiken may suspend, condition, or cancel the provision, delivery, or servicing of the Platform if Kiken has not received a requested end-use certification, if any required government approval has not been obtained, or if Kiken reasonably believes that

an activity may violate applicable Trade Controls or this Section 20. Any violation of this Section 20 constitutes a material breach of this Agreement.

21. ANTI-CORRUPTION

Each party represents and warrants that it has not and will not, in connection with the transactions contemplated by this Agreement, directly or indirectly make, offer, promise, or authorize any payment or transfer of anything of value to any government official, political party, or candidate for political office for the purpose of influencing any act or decision, in violation of the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act, or any other applicable anti-corruption law.

22. DISPUTE RESOLUTION; GOVERNING LAW

22.1 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois, without regard to its conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

22.2 Dispute Resolution

Any dispute arising out of or relating to this Agreement shall first be submitted to good-faith negotiation between senior executives of each party for a period of thirty (30) days. If the dispute is not resolved through negotiation, either party may initiate binding arbitration administered by the American Arbitration Association under its Commercial Arbitration Rules. The arbitration shall be conducted by a single arbitrator in DuPage County, Illinois. The arbitrator's award shall be final and binding, and judgment thereon may be entered in any court of competent jurisdiction.

Any dispute resolution proceeding, whether in arbitration or in court, shall be conducted only on an individual basis and not as a plaintiff or class member in any purported class, collective, consolidated, representative, or private attorney general proceeding. The arbitrator shall have no authority to arbitrate any claim on a class, collective, or representative basis and may not consolidate the claims of more than one party. Each party waives any right to participate in a class, collective, or representative action arising out of or relating to this Agreement. If this waiver of class, collective, and representative proceedings is found to be unenforceable as to a particular claim or request for relief, then that claim or request for relief, and only that claim or request for relief, shall be severed from arbitration and brought in a court of competent jurisdiction, and all remaining claims shall be resolved in arbitration on an individual basis.

22.3 Injunctive Relief

Notwithstanding Section 22.2, either party may seek injunctive or other equitable relief in any court of competent jurisdiction to protect its intellectual property rights or Confidential Information without being required to post a bond or other security.

22.4 Jury Waiver

TO THE FULLEST EXTENT PERMITTED BY LAW, EACH PARTY HEREBY IRREVOCABLY WAIVES ANY RIGHT TO A TRIAL BY JURY IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT.

23. GENERAL PROVISIONS

23.1 Entire Agreement; Integration; Purchase Order Terms

This Agreement, together with all Order Forms and Exhibits, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, representations, and understandings, whether written or oral. **Notwithstanding any terms contained in any Customer purchase order, requisition, or similar document, no terms stated therein other than product name, license quantity (number of Agents), price, Subscription Term, and billing contact shall be incorporated into this Agreement, and all such other terms are expressly rejected and shall have no force or effect on this Agreement.** In the event of any conflict between the body of this Agreement and any Order Form or Exhibit, this Agreement shall control unless the Order Form or Exhibit expressly states that it supersedes a specific provision of this Agreement.

23.2 Amendments

For customers subscribing through Kiken's standard online subscription process, Kiken may update this Agreement from time to time by posting a revised version on its website or providing notice to Customer. Material changes shall be effective thirty (30) days after notice. Continued use of the Platform after such notice constitutes acceptance of the updated terms. For Enterprise Customers, amendments to this Agreement require mutual written consent executed by authorized representatives of both parties.

23.3 Assignment

Neither party may assign this Agreement without the other party's prior written consent, except that either party may assign this Agreement in connection with a merger, acquisition, or sale of all or substantially all of its assets, provided that the assignee agrees to be bound by this Agreement.

23.4 Severability

If any provision of this Agreement is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect, and the invalid provision shall be modified to the minimum extent necessary to make it valid and enforceable while preserving the parties' original intent.

23.5 Waiver

No waiver of any breach of this Agreement shall constitute a waiver of any other or subsequent breach. No waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

23.6 Notices

All notices under this Agreement shall be in writing and shall be deemed given when: (a) delivered personally; (b) sent by confirmed email to the address specified in the Order Form; or (c) one (1) business day after deposit with a nationally recognized overnight courier, addressed to the party at the address specified in the Order Form.

23.7 Independent Contractors

The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, or employment relationship between the parties.

23.8 No Third-Party Beneficiaries

This Agreement is for the sole benefit of the parties and their permitted successors and assigns. Nothing in this Agreement, express or implied, is intended to or shall confer upon any third party any legal or equitable right, benefit, or remedy.

23.9 Counterparts

Order Forms may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one instrument. Electronic signatures shall be deemed valid and binding.

23.10 Order of Precedence

In the event of a conflict among the documents forming this Agreement, the following order of precedence shall apply (highest to lowest): (a) the body of this Agreement; (b) any Exhibits or Addenda; (c) Order Forms; and (d) the Documentation. Notwithstanding the foregoing, an Order Form may expressly supersede a specific provision of this Agreement only if the Order Form specifically identifies the provision being superseded.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

KIKEN TECHNOLOGIES LLC

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER:

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A - SERVICE LEVEL AGREEMENT

1. Platform Availability

Kiken shall use commercially reasonable efforts to maintain Platform availability of at least ninety-nine and nine-tenths percent (99.9%) during each calendar month, measured on a 24x7 basis, excluding Scheduled Maintenance ("**Uptime Commitment**").

2. Scheduled Maintenance

Kiken will provide at least seventy-two (72) hours' prior written notice for scheduled maintenance windows. Scheduled maintenance will be performed during off-peak hours (between 12:00 AM and 6:00 AM Central Time) whenever commercially practicable.

3. Service Credits

If Kiken fails to meet the Uptime Commitment in any calendar month, Customer shall be eligible for service credits as follows: (a) 99.0% to 99.89%: credit equal to ten percent (10%) of monthly fees; (b) 95.0% to 98.99%: credit equal to twenty-five percent (25%) of monthly fees; (c) below 95.0%: credit equal to fifty percent (50%) of monthly fees. Service credits must be requested within thirty (30) days of the applicable month and shall be applied as a credit against future invoices. Service credits shall not exceed fifty percent (50%) of the monthly fees for the applicable month. **Service credits constitute Customer's sole and exclusive remedy, and Kiken's sole and entire liability, for any failure to meet the Uptime Commitment.**

4. Exclusions

The Uptime Commitment does not apply to: (a) Scheduled Maintenance; (b) force majeure events; (c) issues caused by the Customer Environment or Customer's equipment; (d) internet connectivity issues beyond Kiken's control; or (e) Customer's misuse of the Platform.

EXHIBIT B - DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the Agreement and governs the processing of personal data by Kiken on behalf of Customer.

1. Roles

For purposes of applicable data protection and privacy laws, Customer is the controller and Kiken is the processor with respect to personal data processed through the Platform on Customer's behalf. Where the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"), applies, Customer is the business and Kiken is the service provider with respect to such personal information. Kiken shall process such personal data only on Customer's documented instructions and only to the extent necessary to provide the Platform. With respect to Aggregated Data described in Section 9.3 of the Agreement, Kiken acts as an independent controller.

2. Security Measures

Kiken shall implement and maintain appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage, including encryption in transit and at rest, access controls, logging, and regular security assessments.

3. Sub-processors

Kiken may engage sub-processors to assist in providing the Platform, provided that Kiken: (a) maintains a current list of sub-processors available upon request; (b) provides Customer with at least thirty (30) days' prior notice before engaging a new sub-processor; (c) enters into written agreements with sub-processors imposing data protection obligations no less protective than those in this DPA; and (d) remains liable for the acts and omissions of its sub-processors.

4. Data Subject Rights

Kiken shall promptly notify Customer if it receives a request from a data subject exercising rights under applicable data protection laws, and shall provide reasonable assistance to Customer in responding to such requests.

5. Data Breach Notification

Kiken shall notify Customer without undue delay (and in any event within seventy-two (72) hours) upon becoming aware of any personal data breach affecting Customer Data processed through the Platform. Such notification shall include the nature of the breach, the categories and approximate number of data subjects affected, and the measures taken or proposed to be taken to address the breach.

6. California Consumer Privacy Act

To the extent Kiken processes personal information subject to the CCPA on behalf of Customer, Kiken acts as a service provider and shall: (a) not sell or share such personal information; (b) not retain, use, or disclose such personal information for any purpose other

than providing the Platform, or as otherwise permitted by the CCPA; (c) not retain, use, or disclose such personal information outside the direct business relationship between the parties; (d) not combine such personal information with personal information received from another source, except as permitted by the CCPA; and (e) provide the same level of privacy protection as is required of businesses under the CCPA. Kiken certifies that it understands and shall comply with the restrictions set forth in this Section 6.

7. International Transfers

The Platform is operated from, and personal data processed through the Platform on Customer's behalf is hosted within, the United States. If the parties agree that the Platform will be used to process personal data subject to the General Data Protection Regulation, the U.K. GDPR, or the data protection laws of Canada or another jurisdiction outside the United States, Customer remains responsible for establishing a lawful basis for such processing and transfer, and the parties shall enter into such additional terms and transfer mechanisms as may be required, including the European Commission Standard Contractual Clauses or the U.K. International Data Transfer Addendum, which shall be incorporated by reference upon execution of the applicable transfer documentation.

8. Data Return and Deletion

Upon termination of the Agreement, Kiken shall, at Customer's election, return or delete all personal data processed on behalf of Customer, and certify such deletion in writing, subject to applicable legal retention requirements.

EXHIBIT C - SHARED RESPONSIBILITY MATRIX

The following matrix sets forth the allocation of security responsibilities between Kiken and Customer. This matrix is illustrative and does not limit the obligations set forth elsewhere in the Agreement.

KIKEN RESPONSIBILITIES (Platform Security):

Platform infrastructure security, including hosting, network, and physical security

Encryption of Customer Data in transit and at rest within the Platform

Maintenance and patching of Platform software components

Tracer Technology development, maintenance, and updates

DSPM Scanning engine maintenance and threat intelligence updates

Platform access controls and authentication mechanisms

Incident response for security events affecting Platform infrastructure

SOC 2 Type II compliance (or equivalent) for Platform operations

Secure API endpoints and data transmission

Platform backup and disaster recovery

CUSTOMER RESPONSIBILITIES (Environment Security):

Configuration of the Platform, including Tracer Injection and DSPM Scanning parameters

Lawful deployment of the Platform, including authorization to monitor each targeted system and data category and all required notices, consents, and lawful bases

Security of the Customer Environment, including all endpoints, servers, and networks

Management of Authorized User accounts, credentials, and access permissions

Maintenance of firewalls, access controls, and network segmentation within the Customer Environment

Patch management and vulnerability remediation within the Customer Environment

Employee security awareness training

Compliance with applicable laws regarding Tracer deployment and data monitoring

Incident response within the Customer Environment

Evaluation and action upon Platform reports, alerts, and scan results

Maintaining adequate cyber insurance coverage appropriate to Customer's risk profile

Ensuring outbound network connectivity from the Customer Environment to permit Tracer phone-home telemetry functionality

Timely review and update of Configuration as the Customer Environment changes

SHARED RESPONSIBILITIES:

Integration and onboarding of the Platform within the Customer Environment (Kiken provides guidance; Customer implements)

Ongoing communication regarding platform updates, threat intelligence, and configuration best practices

Incident investigation involving both Platform and Customer Environment components