

RealCISO Master Subscription Agreement

This RealCISO Master Subscription Agreement (“MSA”) is a binding agreement between RealCISO Inc., a Delaware corporation (“RealCISO”), and the individual or organization that accepts this MSA by clicking “I Agree,” creating an account, or using the Services (“Customer”) (each a “Party” and together the “Parties”). This MSA is effective as of the date Customer first accepts this MSA or accesses the Services (the “Effective Date”). By accepting this MSA, Customer acknowledges that Customer has read, understood, and agrees to be bound by all terms and conditions herein.

Section 1. Services.

“Services” means the product(s) and service(s) that are ordered by Customer from RealCISO online or through an Order Form referencing this MSA, whether on a trial or paid basis, and to which RealCISO thereby provides access to Customer. Services include any products or services provided by third parties purchased through the RealCISO marketplace, and include AI Services as defined in Section 1A. Subject to the terms and conditions of this MSA, RealCISO will make the Services available during the Term as set forth in an Order Form. In the event of any inconsistency or conflict between the terms of the MSA and the terms of any Order Form, the terms of the Order Form control.

Section 1A. AI Services Definitions.

The following definitions apply to any feature or component of the Services that incorporates artificial intelligence or machine learning capabilities:

1A.1. “AI Services” means any feature, functionality, or component of the Services that uses artificial intelligence, machine learning, natural language processing, large language models, or similar computational techniques to process, analyze, generate, or assist with content, recommendations, assessments, risk scores, or decisions. AI Services include, without limitation: automated risk scoring, compliance gap analysis, remediation recommendations, control mapping suggestions, report generation, and the CLEO AI Assistant (as defined in Section 1A.8), and any other AI-augmented or AI-generated outputs provided through the Services.

1A.8. “CLEO AI Assistant” or “CLEO” means the conversational AI assistant feature within the Services through which Authorized Users may interact with their own Service Data using natural language, including by asking questions about compliance status, generating or modifying tasks and remediation plans, creating or updating reports, and performing other Service functions through conversational prompts. CLEO processes Customer’s Service Data solely on Customer’s behalf for Customer’s own benefit. RealCISO does not use Service Data processed by CLEO as training data for AI Models shared across other customers.

1A.2. “AI Model” means any machine learning model, algorithm, neural network, large language model, or statistical model used by RealCISO to provide AI Services, including any pre-trained, fine-tuned, or custom-developed models, whether developed by RealCISO or licensed from third-party providers.

1A.3. “AI Output” means any content, recommendation, analysis, score, assessment, report, mapping, remediation plan, or other output generated or materially assisted by AI Services. AI Outputs are provided as decision-support tools and do not constitute legal, regulatory, compliance, or other professional advice.

1A.4. “Automated Decision” means any decision made by the AI Services without contemporaneous human review that produces legal effects or similarly significant effects concerning the Customer, its Authorized Users, or its end users, including but not limited to compliance risk classifications, audit findings, or remediation prioritizations that are acted upon without human validation.

1A.5. “High-Risk AI Use” means any use of AI Services that: (a) constitutes a “high-risk artificial intelligence system” under the Colorado Artificial Intelligence Act (SB 24-205); (b) involves Automated Decisions that materially affect an individual’s access to employment, credit, insurance, housing, education, or essential services; or (c) is classified as high-risk under any other applicable AI-specific law or regulation (including any International AI Compliance Addendum executed by the Parties).

1A.6. “AI Acceptable Use Policy” means the policy published by RealCISO at <https://www.realciso.io/legal/ai-aup> (as updated from time to time) setting forth permitted and prohibited uses of AI Services, which is incorporated into this MSA by reference.

Section 2. Fees and Payment.

2.1. Fees. Customer will pay the fees specified in the Order Form or as outlined on the Usage Plan page for Affiliates or Billing page for all other licenses (the “Fees”).

2.2. Payment; Taxes. RealCISO will invoice Customer for Fees, either within the Services or directly, within thirty (30) days of the Effective Date. Customer will pay all invoiced fees as outlined in the Fees as described in Section 2.1. Any late payments are subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less. Fees do not include local, state, or federal taxes or duties of any kind and any such taxes will be assumed and paid by Customer, except for taxes on RealCISO based on RealCISO’s income or receipts.

Section 3. Term and Termination.

3.1. Term. This MSA commences on the Effective Date and will remain in effect through the Initial Term and all Renewal Terms, as specified in the Order Form, unless otherwise terminated in accordance with this Section (the Initial Term and all Renewal Terms collectively the “Term”). If the Order Form does not specify, the Initial Term will be one year and will automatically renew for successive one-year periods unless a Party provides notice of non-renewal in accordance with Section 3.3.

3.2. Termination for Cause. A Party may terminate this MSA for cause (a) upon notice to the other Party of a material breach if such breach remains uncured after fifteen (15) days from the date of the breaching Party’s receipt of such notice; or (b) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Non-payment of Fees by Customer past ninety (90) days from an invoice date, any Prohibited Uses (as defined below), and any violation of the AI Acceptable Use Policy will be considered de facto material breaches of the MSA.

3.3. Cancellation. A Party may terminate the MSA and an applicable Order Form either (i) in accordance with the renewal provisions of the Order Form or (ii) if such provisions are not specified, by providing written notice of termination to the other Party at least sixty (60) days prior to the end of the then-current Term. A timely notice of termination under this Section also constitutes notice of non-renewal and prevents any Renewal Term from commencing at the end of the current Term. For clarity: a notice of termination delivered with fewer than sixty (60) days remaining in the current Term does not cancel the current Term, does not prevent the commencement of the immediately following Renewal Term, and does not entitle Customer to a

refund of any pre-paid Fees for that Renewal Term; it will, however, prevent any further auto-renewal after that Renewal Term expires if sixty (60) or more days remain before that Renewal Term's end at the time the notice is received.

3.4. Effect of Termination and Survival. Upon termination or cancellation of an Order Form or this MSA (a) with respect to termination of the entire MSA, all Order Forms will concurrently terminate, (b) Customer will have no further right to use the Services under the terminated or cancelled Order Forms and RealCISO will remove Customer's access to same, and (c) unless otherwise specified in writing, Customer will not be entitled to any refund of fees paid. The following Sections will survive termination: Section 2 (Fees and Payment), Section 5 (Confidentiality), Section 6.2 (Data Practices—Ownership), Section 6.5 (AI Data Processing), Section 8 (Intellectual Property Rights), Section 9.3 (Disclaimers), Section 9.4 (AI Service Disclaimers), Section 10 (Indemnification), Section 11 (Limitation of Liability), Section 12 (Miscellaneous), and Section 13 (AI Governance and Transparency) to the extent obligations therein relate to data processing, ownership, or compliance obligations that arise or accrue during the Term. For the avoidance of doubt, Section 6.5.1 (No Training on Customer Data) survives termination. Termination of this MSA will not limit a Party's liability for obligations accrued as of or prior to such termination or for any breach of this MSA.

Section 4. License and Use of the Services.

4.1. License. RealCISO hereby grants Customer a non-exclusive, non-transferable, sublicensable right to and license to access and use the Services (including AI Services) set forth in the Order Form for Customer's internal business purposes or for the benefit of Customer's end customer, all subject to the terms and conditions of this MSA, the Order Form, and the AI Acceptable Use Policy.

4.2. Authorized Users. Customer may designate and provide access to its (or its corporate affiliates') employees, independent contractors, or other agents to an account on the Services as authorized users (each an "Authorized User") up to the number of "seats" set forth in the Order Form (unlimited if not specified in the Order Form). Each account may be used only by a single, individual Authorized User, and Customer may be charged for additional seats (if applicable), or RealCISO may terminate the MSA for cause, if this requirement is circumvented. Customer is responsible for all use and misuse of the Services by Authorized User accounts and for adherence to this MSA by any Authorized Users, and references to Customer herein will be deemed to apply to Authorized Users as necessary and applicable. Customer agrees to promptly notify RealCISO of any unauthorized access or use of which Customer becomes aware.

4.3. Prohibited Uses. Customer and Authorized Users will not:

- (a) "frame," distribute, resell, or permit access to the Services by any third party other than for its intended purposes;
- (b) use the Services other than in compliance with applicable federal, state, and local laws;
- (c) interfere with the Services or disrupt any other user's access to the Subscription Service;
- (d) reverse engineer, attempt to gain unauthorized access to the Service, attempt to discover the underlying source code or structure of, or otherwise copy or attempt to copy the Services;
- (e) knowingly transfer to the Services any content or data that is defamatory, harassing, discriminatory, infringing of third party intellectual property rights, or unlawful;

- (f) transfer to the Services or otherwise use on the Services any routine, device, code, exploit, or other undisclosed feature that is designed to delete, disable, deactivate, interfere with or otherwise harm any software, program, data, device, system or service, or which is intended to provide unauthorized access or to produce unauthorized modifications;
- (g) use any robot, spider, data scraping, or extraction tool or similar mechanism with respect to the Services;
- (h) use AI Outputs as the sole or determinative basis for any legal, regulatory, compliance, employment, or other decision that produces legal or similarly significant effects on any individual without qualified human review and oversight;
- (i) introduce adversarial inputs, prompt injection attacks, jailbreaking techniques, or other methods designed to manipulate, extract proprietary information from, or circumvent the safety mechanisms of AI Services;
- (j) use AI Services to generate content that impersonates individuals, creates misleading compliance documentation, fabricates evidence of regulatory compliance, or produces fraudulent audit artifacts;
- (k) attempt to reverse engineer, extract, distill, replicate, or derive the AI Models, their weights, training data, or architecture through any means, including systematic querying, output analysis, or model inversion techniques;
- (l) use AI Services for any purpose that would constitute a High-Risk AI Use under applicable law without first: (i) notifying RealCISO of such intended use; (ii) conducting or obtaining an AI impact assessment; and (iii) implementing the additional safeguards specified in Section 13 (AI Governance and Transparency);
- (m) use AI Services to process categories of data that AI Services are not designed to handle, including but not limited to protected health information (PHI) subject to HIPAA unless a Business Associate Agreement is in place, or payment card data subject to PCI-DSS; or
- (n) represent AI Outputs to any third party, regulator, or auditor as having been produced by a qualified human professional without disclosing the AI-assisted nature of such outputs.

Section 5. Confidentiality.

As used herein, the “Confidential Information” of a Party (the “Disclosing Party”) means all financial, technical, or business information of the Disclosing Party that the Disclosing Party designates as confidential at the time of disclosure to the other Party (the “Receiving Party”) or that the Receiving Party reasonably should understand to be confidential based on the nature of the information or the circumstances surrounding its disclosure. For the sake of clarity, the Parties acknowledge that Confidential Information includes the terms and conditions of this MSA, AI Model documentation provided under Section 13.2, and any bias testing results disclosed under Section 13.4. Except as expressly permitted in this MSA, the Receiving Party will not disclose, duplicate, publish, transfer or otherwise make available Confidential Information of the Disclosing Party in any form to any person or entity without the Disclosing Party’s prior written consent. The Receiving Party will not use the Disclosing Party’s Confidential Information except to perform its obligations under this MSA, such obligations including, in the case of RealCISO, to provide the Services. Notwithstanding the foregoing, the Receiving Party may disclose Confidential Information to the extent required by law, provided that the Receiving Party: (a) gives the Disclosing Party prior written notice of such disclosure so as to afford the Disclosing Party a reasonable opportunity to appear, object, and obtain a protective order or other appropriate relief regarding such disclosure (if such notice is not prohibited by applicable

law); (b) uses diligent efforts to limit disclosure and to obtain confidential treatment or a protective order; and (c) allows the Disclosing Party to participate in the proceeding. Further, Confidential Information does not include any information that: (i) is or becomes generally known to the public without the Receiving Party's breach of any obligation owed to the Disclosing Party; (ii) was independently developed by the Receiving Party without the Receiving Party's breach of any obligation owed to the Disclosing Party; or (iii) is received from a third party who obtained such Confidential Information without any third party's breach of any obligation owed to the Disclosing Party.

Section 6. Data Practices.

6.1. Definitions. "Service Data" means a subset of Confidential Information comprised of electronic data, text, messages, communications, or other materials submitted to and stored within the Services by Customer in connection with use of the Services. Service Data may include, without limitation, any information relating to an identified or identifiable natural person ('data subject') where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity of that natural person (such information, "Personal Data"). Service Data does not include metrics and information regarding Customer's use of the Services, including information about how Authorized Users use the Services (such information, "Usage Data").

6.2. Ownership. Customer will continue to retain its ownership rights to all Service Data processed under the terms of this MSA and RealCISO will own all Usage Data.

6.3. RealCISO's Use of Data. RealCISO will use Service Data, Personal Data, and Usage Data as follows and, to the extent necessary, Customer provides RealCISO a license to use, modify, reproduce, distribute, display and disclose same during the Term in accordance with this MSA:

6.3.1. Operating the Services. RealCISO may receive, collect, store and/or process Service Data based on RealCISO's legitimate interest in operating the Services. For example, RealCISO may collect Personal Data (such as name, phone number, or credit card information) through the account activation process. RealCISO will use Service Data solely to provide, operate, secure, and improve the Services for Customer's benefit. RealCISO will not use Customer's Service Data to train AI Models, and any use of aggregated or anonymized usage patterns to improve the Services is governed by Section 6.5.

6.3.2. Communications. RealCISO may communicate with Customer or Authorized Users (i) to send product information and promotional offers or (ii) about the Services generally. If Customer or an Authorized User does not want to receive such communications, Customer may email support@realciso.io. Customer and necessary Authorized Users will always receive transactional messages that are required for RealCISO to provide the Services (such as billing notices and product usage notifications).

6.3.3. Improving the Services. RealCISO may collect, and may engage third-party analytics providers to collect, Usage Data to develop new features, improve existing features, or inform sales and marketing strategies based on RealCISO's legitimate interest in improving the Services. When RealCISO uses Usage Data, any Personal Data that was included in Service Data shall be anonymized and/or aggregated in such a manner that it no longer constitutes Service Data or Personal Data under applicable data protection laws. Any such third-party analytics providers will not share or otherwise disclose Usage Data, although RealCISO may make Usage Data publicly available from time to time.

6.3.4. Third-Party Service Providers. Customer agrees that RealCISO may provide Service Data and Personal Data to authorized third-party service providers, only to the extent necessary to provide, secure, or improve the Services. Any such third-party service providers will only be given access to Service Data and Personal Data as is reasonably necessary to provide the Services and will be subject to (a) confidentiality obligations which are commercially reasonable and substantially consistent with the standards described in this MSA; and (b) their agreement to comply with the data transfer restrictions applicable to Personal Data as set forth below.

6.4. Service Data Safeguards. (i) RealCISO will not sell, rent, or lease Service Data to any third party, and will not share Service Data with third parties, except as permitted by this MSA and to provide, secure, and support the Services. (ii) RealCISO will maintain commercially reasonable (particularly for a company of RealCISO's size and revenue) appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Service Data.

6.5. AI Data Processing.

6.5.1. No Training on Customer Data. RealCISO does not use Customer's Service Data to train, fine-tune, validate, or otherwise develop AI Models, including any AI Models used to provide AI Services to other customers. AI Services process Customer's Service Data solely to deliver the Services to Customer as described in the applicable Order Form. RealCISO will not use Personal Data (as defined in Section 6.1) for any AI model development purpose. Nothing in this Section restricts RealCISO's use of fully anonymized and aggregated Usage Data (which cannot be re-identified to Customer or any individual) to monitor and improve platform performance, as governed by Section 6.3.3.

6.5.2. AI Data Isolation. When processing Service Data through AI Services, RealCISO will maintain logical separation between Customer's Service Data and data belonging to other customers. Customer's Service Data will not be used to generate AI Outputs for, or improve the service quality provided to, any other customer.

6.5.3. AI Processing Transparency. Upon Customer's written request (no more than once per calendar quarter), RealCISO will provide a summary description of: (a) the categories of Service Data processed by AI Services; (b) the purposes for which AI Services process such data; (c) the types of AI Models used; (d) any third-party AI sub-processors involved in delivering AI Services; and (e) the jurisdictions in which AI processing occurs.

6.5.4. Automated Decision-Making Disclosure. To the extent AI Services make or materially support Automated Decisions as defined in Section 1A: (a) RealCISO will clearly identify such features in the Services documentation and user interface; (b) RealCISO will provide Customer with the ability to request human review of any Automated Decision; (c) RealCISO will provide mechanisms for Customer to opt out of Automated Decision-making where required by applicable law (including California Consumer Privacy Act regulations regarding Automated Decision-Making Technology); and (d) RealCISO will maintain records sufficient to explain the principal factors contributing to any Automated Decision for a minimum of twelve (12) months.

6.5.5. AI Sub-Processors. In addition to the Sub-Processor obligations in Section 7.3, RealCISO will: (a) identify any third-party AI model providers (including foundation model providers and embedding service providers) in its Sub-Processor list; (b) contractually prohibit any third-party AI model provider from retaining or using Customer's Service Data for that provider's own purposes, including model training; and (c) provide Customer with thirty (30) days' prior written notice before engaging a new AI sub-processor, during which period Customer may object in writing and, if not resolved within fifteen (15) days, terminate the affected Order Form without penalty.

6.5.6. Data Deletion. Upon termination of this MSA or an applicable Order Form, or upon Customer's written request, RealCISO will delete or return (at Customer's election) all Service Data within thirty (30) days, except to the extent retention is required by applicable law. RealCISO will certify in writing that such deletion has been completed.

6.5.7. AI Audit Rights. Customer (or its designated independent third-party auditor, subject to reasonable confidentiality obligations) may, upon thirty (30) days' written notice and no more than once per calendar year, audit RealCISO's compliance with this Section 6.5. Such audit will be conducted during normal business hours, will not unreasonably interfere with RealCISO's operations, and will be at Customer's expense. RealCISO will cooperate reasonably with such audit and provide access to relevant records and personnel.

6.5.8. CLEO AI Assistant Controls. The CLEO AI Assistant is an AI Service feature that processes Customer's Service Data solely within Customer's account to respond to Authorized User requests. Customer may control CLEO access as follows: (a) Disable CLEO. Customer's designated administrator may disable the CLEO AI Assistant for the entire account or for individual user roles through the platform's Settings menu (Settings > AI Features > CLEO). Disabling CLEO does not affect access to any other AI Services or non-AI features of the platform. (b) Re-enablement. Customer may re-enable CLEO at any time through the same platform settings. RealCISO will restore full CLEO functionality within one (1) business day of re-enablement. (c) Effect on Service. Disabling CLEO will prevent Authorized Users from submitting natural language queries, generating or modifying tasks through conversational interface, or accessing CLEO-specific report generation features. All other platform features, including non-AI compliance assessment, remediation tracking, and reporting, will continue without interruption.

Section 7. Privacy Practices.

7.1. Privacy Policy. RealCISO operates the Services and, as applicable, handles Personal Data, pursuant to the privacy policy available at <https://www.realciso.io/privacy-policy/> (the "Privacy Policy").

7.2. Customer as Controller. To the extent Service Data constitutes Personal Data, the Parties agree that Customer determines the purpose and means of processing such Personal Data, and RealCISO processes such information on behalf of Customer.

7.3. Hosting and Processing. Unless otherwise specifically agreed to by RealCISO, Service Data may be hosted by RealCISO, or its respective authorized third-party service providers, in the United States or other locations around the world. In providing the Services, RealCISO will engage entities to process Service Data, including and without limitation, any Personal Data within Service Data pursuant to this MSA, within the United States and in other countries and territories.

7.4. Sub-Processors. Customer acknowledges and agrees that RealCISO may use third-party data processors engaged by RealCISO who receive Service Data from RealCISO for processing on behalf of Customer and in accordance with Customer's instructions (as communicated by RealCISO) and the terms of its written subcontract (the "Sub-Processors"). Such Sub-Processors may access Service Data to provide, secure, and improve the Services. RealCISO will be responsible for the acts and omissions of Sub-Processors to the same extent that RealCISO would be responsible if RealCISO was performing the services directly under the terms of this MSA. The names and locations of all current Sub-Processors used for the processing of Personal Data under this MSA, if any, are set forth in the Privacy Policy.

Section 8. Intellectual Property Rights.

8.1. General IP. Each Party will retain all rights, title and interest in any patents, inventions, copyrights, trademarks, domain names, trade secrets, know-how and any other intellectual property and/or proprietary rights (“Intellectual Property Rights”), and RealCISO in particular will exclusively retain such rights in the Services and all components of or used to provide the Services.

8.2. Feedback License. Customer hereby provides RealCISO a fully paid-up, royalty-free, worldwide, transferable, sub-licensable (through multiple layers), assignable, irrevocable and perpetual license to implement, use, modify, commercially exploit, incorporate into the Services or otherwise use any suggestions, enhancement requests, recommendations or other feedback RealCISO receives from Customer, Customer’s agents or representatives, Authorized Users, or other third parties acting on Customer’s behalf; and RealCISO also reserves the right to seek intellectual property protection for any features, functionality or components that may be based on or that were initiated by such suggestions, enhancement requests, recommendations or other feedback, subject to the limitations in Section 8.5.

8.3. AI Output Ownership. As between the Parties, Customer will own all AI Outputs generated using Customer’s Service Data through the AI Services, subject to RealCISO’s retained Intellectual Property Rights in the underlying AI Models, algorithms, and pre-trained components. RealCISO retains no rights to the specific content of AI Outputs generated for Customer. The Parties acknowledge that AI Outputs may not be eligible for copyright protection under applicable law, and this ownership allocation is a contractual assignment of whatever rights may exist.

8.4. AI Model IP. RealCISO exclusively retains all Intellectual Property Rights in its AI Models, including all weights, parameters, architectures, training methodologies, and pre-trained components. Nothing in this MSA grants Customer any rights to the AI Models themselves, distinct from the right to use the AI Services as provided herein.

8.5. Feedback Limitation for AI. Notwithstanding the feedback license granted in Section 8.2: (a) Customer’s feedback regarding AI Services will not be used to train AI Models in a manner that would directly compete with Customer’s core business; (b) Customer’s proprietary workflows, assessment methodologies, or compliance frameworks submitted as Service Data will not be extracted or replicated for the benefit of other customers without Customer’s written consent; and (c) this limitation does not restrict RealCISO’s ability to use feedback to improve AI Services generally, including for bias remediation, safety improvements, and accuracy enhancements that benefit all customers.

Section 9. Representations, Warranties, and Disclaimers.

9.1. Authority. Each Party represents that it has validly entered into this MSA and has the legal power to do so.

9.2. Warranties. RealCISO warrants that during an applicable Term (a) this MSA will accurately describe the applicable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Service Data; and (b) the Services will perform materially in accordance with the applicable documentation provided within the Services. For any breach of a warranty in this section, Customer’s exclusive remedies are those described in Section 3 (Term and Termination) herein.

9.3. Disclaimers. EXCEPT AS SPECIFICALLY SET FORTH IN THIS SECTION AND ANY APPLICABLE SERVICE LEVEL AGREEMENT, THE SERVICES, INCLUDING ALL SERVER AND NETWORK COMPONENTS, ARE PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS, WITHOUT ANY WARRANTIES OF ANY KIND TO THE FULLEST EXTENT

PERMITTED BY LAW, AND REALCISO EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CUSTOMER ACKNOWLEDGES THAT REALCISO DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, ERROR-FREE, OR FREE FROM VIRUSES OR OTHER MALICIOUS SOFTWARE, AND NO INFORMATION OR ADVICE OBTAINED BY CUSTOMER FROM REALCISO OR THROUGH THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS MSA. THE PARTIES ADDITIONALLY AGREE THAT REALCISO WILL HAVE NO LIABILITY OR RESPONSIBILITY FOR CUSTOMER'S VARIOUS COMPLIANCE PROGRAMS, AND THAT THE SERVICES, TO THE EXTENT APPLICABLE, ARE ONLY TOOLS FOR ASSISTING CUSTOMER IN MEETING THE VARIOUS COMPLIANCE OBLIGATIONS FOR WHICH IT SOLELY IS RESPONSIBLE.

9.4. AI Service Disclaimers. IN ADDITION TO THE DISCLAIMERS IN SECTION 9.3, CUSTOMER ACKNOWLEDGES AND AGREES THAT:

(a) AI OUTPUTS ARE GENERATED BY MACHINE LEARNING MODELS AND MAY CONTAIN ERRORS, INACCURACIES, OMISSIONS, HALLUCINATIONS, OR OUTDATED INFORMATION. AI OUTPUTS DO NOT CONSTITUTE LEGAL, REGULATORY, COMPLIANCE, OR PROFESSIONAL ADVICE OF ANY KIND;

(b) AI SERVICES ARE DECISION-SUPPORT TOOLS ONLY. CUSTOMER IS SOLELY RESPONSIBLE FOR REVIEWING, VALIDATING, AND APPROVING ALL AI OUTPUTS BEFORE RELYING UPON THEM FOR ANY PURPOSE, INCLUDING BUT NOT LIMITED TO COMPLIANCE DECISIONS, REGULATORY SUBMISSIONS, AUDIT RESPONSES, AND RISK ASSESSMENTS;

(c) AI MODELS MAY PRODUCE DIFFERENT OUTPUTS FROM THE SAME OR SIMILAR INPUTS AND MAY REFLECT BIASES PRESENT IN TRAINING DATA OR MODEL ARCHITECTURE. REALCISO DOES NOT WARRANT THAT AI OUTPUTS WILL BE FREE FROM BIAS, STATISTICALLY REPRESENTATIVE, COMPLETE, OR SUITABLE FOR ANY PARTICULAR REGULATORY SUBMISSION OR AUDIT PURPOSE;

(d) AI SERVICES MAY BE UPDATED, MODIFIED, OR RETRAINED FROM TIME TO TIME IN ACCORDANCE WITH SECTION 13.5, WHICH MAY ALTER THE NATURE, QUALITY, OR BEHAVIOR OF AI OUTPUTS;

(e) CUSTOMER'S COMPLIANCE OBLIGATIONS UNDER APPLICABLE LAW (INCLUDING ANY FRAMEWORK ASSESSED THROUGH THE SERVICES) REMAIN SOLELY CUSTOMER'S RESPONSIBILITY. REALCISO IS NOT LIABLE FOR ANY REGULATORY NON-COMPLIANCE, AUDIT FAILURE, OR ENFORCEMENT ACTION RESULTING FROM CUSTOMER'S RELIANCE ON AI OUTPUTS WITHOUT INDEPENDENT VERIFICATION BY QUALIFIED PROFESSIONALS; AND

(f) THE AVAILABILITY, ACCURACY, AND FUNCTIONALITY OF AI SERVICES MAY VARY BASED ON THE QUALITY, COMPLETENESS, AND FORMAT OF SERVICE DATA PROVIDED BY CUSTOMER. REALCISO IS NOT RESPONSIBLE FOR AI OUTPUT QUALITY DEGRADATION CAUSED BY INCOMPLETE, INACCURATE, OR IMPROPERLY FORMATTED CUSTOMER DATA.

Section 10. Indemnification.

10.1. Indemnification by RealCISO. RealCISO will indemnify and hold Customer harmless from and against any claim brought by a third party against Customer by reason of Customer's

use of a Service as permitted hereunder, alleging that such Service infringes or misappropriates a third party's valid patent, copyright, trademark, or trade secret (an "IP Claim"). RealCISO will, at its expense, defend such IP Claim and pay damages finally awarded against Customer in connection therewith, including the reasonable fees and expenses of the attorneys engaged by RealCISO for such defense, provided that (a) Customer promptly notifies RealCISO of the threat or notice of such IP Claim; (b) RealCISO will have the sole and exclusive control and authority to select defense attorneys, and defend and/or settle any such IP Claim (however, RealCISO will not settle or compromise any claim that results in liability or admission of any liability by Customer without prior written consent); and (c) Customer fully cooperates with RealCISO in connection therewith. If use of a Service by Customer has become, or, in RealCISO's opinion, is likely to become, the subject of any such IP Claim, RealCISO may, at its option and expense, (i) procure for Customer the right to continue using the Service(s) as set forth hereunder; (ii) replace or modify a Service to make it non-infringing; or (iii) if options (i) or (ii) are not commercially reasonable or practicable as determined by RealCISO, terminate Customer's subscription to the Service(s) and repay, on a pro-rata basis, any Fees previously paid to RealCISO for the corresponding unused portion of the Term for such Service(s). RealCISO will have no liability or obligation under this Section with respect to any IP Claim if such claim is caused in whole or in part by (x) compliance with designs, data, instructions or specifications provided by Customer; (y) modification of the Service(s) by anyone other than RealCISO; or (z) the combination, operation or use of the Service(s) with other hardware or software where a Service would not by itself be infringing. The provisions of this Section state the sole, exclusive, and entire liability of RealCISO to Customer and constitute Customer's sole remedy with respect to an IP Claim brought by reason of access to or use of a Service by Customer, Customer's agents, or Authorized Users.

10.2. Indemnification by Customer. Customer will indemnify and hold RealCISO harmless against any claim (a) arising from or related to use of a Service by Customer, Customer's agents, or Authorized Users in breach of this MSA; or (b) alleging that Customer's use of the Service or Customer's Service Data infringes or misappropriates a third party's valid patent, copyright, trademark, or trade secret; provided (i) RealCISO promptly notifies Customer of the threat or notice of such claim; (ii) Customer will have the sole and exclusive control and authority to select defense attorneys, and defend and/or settle any such claim (however, Customer will not settle or compromise any claim that results in liability or admission of any liability by RealCISO without prior written consent); and (iii) RealCISO fully cooperates in connection therewith.

10.3. Customer Indemnification for AI Misuse. In addition to Customer's indemnification obligations in Section 10.2, Customer will indemnify and hold RealCISO harmless against any claim arising from: (a) Customer's use of AI Outputs as the sole basis for decisions producing legal or similarly significant effects without the human review required by Section 4.3(h); (b) Customer's failure to comply with Automated Decision-Making disclosure, notice, or opt-out requirements applicable to Customer's use of the AI Services under applicable law; (c) Customer's use of AI Services in violation of the Prohibited Uses set forth in Section 4.3(h)–(n) or the AI Acceptable Use Policy; or (d) Customer's representation of AI Outputs as the work of a qualified human professional in violation of Section 4.3(n). This indemnification does not apply to the extent the underlying claim results from RealCISO's gross negligence, willful misconduct, or RealCISO's failure to perform its obligations under Sections 6.5 or 13.

10.4. AI Incident Notification. Each Party will notify the other Party within seventy-two (72) hours of becoming aware of any AI-related security incident, data breach involving AI-processed Service Data, or material AI system failure that affects or is reasonably likely to affect the other Party or its end users.

SECTION 11. LIMITATION OF LIABILITY.

11.1. GENERAL LIMITATION. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE) WILL EITHER PARTY TO THIS MSA, OR THEIR AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SERVICE PROVIDERS, SUPPLIERS OR LICENSORS BE LIABLE TO THE OTHER PARTY OR ANY AFFILIATE FOR ANY LOST PROFITS, LOST SALES OR BUSINESS, LOST DATA (BEING DATA LOST IN THE COURSE OF TRANSMISSION VIA CUSTOMER'S SYSTEMS OR OVER THE INTERNET THROUGH NO FAULT OF REALCISO), BUSINESS INTERRUPTION, LOSS OF GOODWILL, COSTS OF COVER OR REPLACEMENT, OR FOR ANY TYPE OF INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR PUNITIVE LOSS OR DAMAGES, OR ANY OTHER INDIRECT LOSS OR DAMAGES INCURRED BY THE OTHER PARTY OR ANY AFFILIATE IN CONNECTION WITH THIS MSA OR THE SERVICES REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF OR COULD HAVE FORESEEN SUCH DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS MSA, REALCISO'S AGGREGATE LIABILITY TO CUSTOMER, ANY CUSTOMER AFFILIATE, OR ANY THIRD PARTY ARISING OUT OF THIS MSA OR THE SERVICES WILL IN NO EVENT EXCEED THE FEES PAID BY CUSTOMER DURING THE TWELVE (12) MONTHS PRIOR TO THE FIRST EVENT OR OCCURRENCE GIVING RISE TO SUCH LIABILITY. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE ESSENTIAL PURPOSE OF THIS SECTION IS TO ALLOCATE THE RISKS UNDER THIS MSA BETWEEN THE PARTIES AND LIMIT POTENTIAL LIABILITY GIVEN THE FEES, WHICH WOULD HAVE BEEN SUBSTANTIALLY HIGHER IF REALCISO WERE TO ASSUME ANY FURTHER LIABILITY OTHER THAN AS SET FORTH HEREIN. REALCISO HAS RELIED ON THESE LIMITATIONS IN DETERMINING WHETHER TO PROVIDE CUSTOMER WITH THE RIGHTS TO ACCESS AND USE THE SERVICES PROVIDED FOR IN THIS MSA. THE LIMITATION OF LIABILITY PROVIDED FOR HEREIN WILL APPLY IN AGGREGATE TO SUBSCRIBER AND ITS AFFILIATES AND SHALL NOT BE CUMULATIVE.

11.2. AI-SPECIFIC LIABILITY. THE FOLLOWING CLAIMS ARE EXCLUDED FROM THE GENERAL LIABILITY CAP IN SECTION 11.1 AND SHALL INSTEAD BE SUBJECT TO A MAXIMUM AGGREGATE LIABILITY EQUAL TO TWO TIMES (2x) THE FEES PAID BY CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE FIRST EVENT GIVING RISE TO SUCH LIABILITY: (A) CLAIMS ARISING FROM REALCISO'S MATERIAL BREACH OF SECTION 6.5 (AI DATA PROCESSING), INCLUDING UNAUTHORIZED USE OF CUSTOMER SERVICE DATA FOR AI MODEL TRAINING IN VIOLATION OF SECTION 6.5.1; AND (B) CLAIMS ARISING FROM REALCISO'S MATERIAL BREACH OF ITS OBLIGATIONS UNDER SECTION 13 (AI GOVERNANCE AND TRANSPARENCY) THAT CONTINUES UNCURED FOR THIRTY (30) OR MORE CONSECUTIVE DAYS AFTER WRITTEN NOTICE FROM CUSTOMER. FOR CLARITY, "MATERIAL BREACH" FOR PURPOSES OF THIS SECTION 11.2 MEANS A BREACH THAT IS NOT DE MINIMIS AND THAT HAS A DEMONSTRABLE ADVERSE EFFECT ON CUSTOMER'S USE OF AI SERVICES OR CUSTOMER'S REGULATORY COMPLIANCE POSTURE.

11.3. EXCLUSIONS. THE LIMITATIONS SET FORTH IN SECTIONS 11.1 AND 11.2 SHALL NOT APPLY TO: (A) CLAIMS OR DAMAGES RESULTING FROM REALCISO'S IP CLAIMS INDEMNITY OBLIGATIONS IN THIS MSA; (B) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (C) EITHER PARTY'S BREACH OF SECTION 5 (CONFIDENTIALITY) WITH RESPECT TO THE OTHER PARTY'S CONFIDENTIAL INFORMATION.

Some jurisdictions do not allow the exclusion of implied warranties or limitation of liability for incidental or consequential damages or for personal injury or death, which means that some of the above limitations may not apply to Customer. IN THESE JURISDICTIONS, REALCISO'S LIABILITY WILL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY LAW. Any claims or damages that Customer may have against RealCISO will only be enforceable against RealCISO and not any other entity or its officers, directors, representatives, or agents.

Section 12. Miscellaneous.

12.1. Entire Agreement. This MSA, the applicable Order Form(s), and the AI Acceptable Use Policy (incorporated herein by reference) constitute the entire agreement, and supersede all prior agreements, between RealCISO and Customer regarding the subject matter hereof.

12.2. Assignment. Either Party may, without the consent of the other Party, assign this MSA to any affiliate or in connection with any merger, change of control, or the sale of all or substantially all of such Party's assets provided that (1) the other Party is provided prior notice of such assignment and (2) any such successor agrees to fulfill its obligations pursuant to this MSA. Subject to the foregoing restrictions, this MSA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns.

12.3. Severability. If any provision in this MSA is held by a court of competent jurisdiction to be unenforceable, such provision will be modified by the court and interpreted so as to best accomplish the original provision to the fullest extent permitted by law, and the remaining provisions of this MSA will remain in effect.

12.4. Relationship of the Parties. The Parties are independent contractors. This MSA does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

12.5. Notices. All notices provided by RealCISO to Customer under this MSA may be delivered in writing (a) by nationally recognized overnight delivery service ("Courier") or U.S. mail to the contact mailing address provided by Customer on the Order Form; or (b) electronic mail to the electronic mail address provided for Customer's account owner. Customer must give notice to RealCISO in writing. All notices shall be deemed to have been given immediately upon delivery by electronic mail; or, if otherwise delivered upon the earlier of receipt or two (2) business days after being deposited in the mail or with a Courier as permitted above.

12.6. Governing Law, Jurisdiction, Venue. This MSA will be governed by the laws of the State of Massachusetts, without reference to conflict of laws principles. Any disputes under this MSA shall be resolved in a court of general jurisdiction in Worcester County, Massachusetts. Customer hereby expressly agrees to submit to the exclusive personal jurisdiction and venue of such courts for the purpose of resolving any dispute relating to this MSA or access to or use of the Services by Customer, its agents, or Authorized Users.

12.7. Publicity and Marketing. RealCISO may use Customer's name, logo, and trademarks solely to identify Customer as a client of RealCISO on RealCISO's website and other marketing materials and in accordance with Customer's trademark usage guidelines, if Customer provides same to RealCISO. RealCISO may share aggregated and/or anonymized information regarding use of the Services with third parties for marketing purposes to develop and promote Services. RealCISO never will disclose aggregated and/or anonymized information to a third party in a manner that would identify Customer as the source of the information or Authorized Users or others personally.

12.8. Amendments. RealCISO may amend this MSA from time to time, in which case the new MSA will supersede prior versions. RealCISO will notify Customer not less than ten (10) days

prior to the effective date of any such amendment and Customer's continued use of the Services following the effective date of any such amendment may be relied upon by RealCISO as consent to any such amendment. For amendments to Sections 6.5, 8.3–8.5, 9.4, or 13 that materially reduce Customer's rights or materially expand RealCISO's rights with respect to AI Services, RealCISO will provide not less than thirty (30) days' prior written notice. RealCISO's failure to enforce at any time any provision of this MSA does not constitute a waiver of that provision or of any other provision of this MSA.

12.9. Electronic Acceptance. This MSA is a click-through agreement presented during the RealCISO account creation process. By clicking "I Agree," "Accept," or a similar button, or by creating an account, accessing, or using the Services, Customer agrees to be bound by this MSA. If Customer is accepting this MSA on behalf of an organization, Customer represents and warrants that Customer has the authority to bind such organization to this MSA. If Customer does not agree to this MSA, Customer must not create an account or use the Services. This MSA applies to Customer if: (a) Customer creates a new account on or after May 1, 2026; (b) Customer enters into a Trial of RealCISO that references this MSA; or (c) Customer clicks a button indicating agreement with this MSA, enters into an Order Form, or otherwise accepts these terms electronically. Each Party agrees that electronic acceptance constitutes a valid and binding agreement under the Electronic Signatures in Global and National Commerce Act (E-SIGN Act, 15 U.S.C. §7001 et seq.) and the Uniform Electronic Transactions Act (UETA), and is enforceable to the same extent as a manually signed agreement.

Section 13. AI Governance and Transparency.

13.1. AI Governance Framework. RealCISO will maintain an AI governance framework aligned with the NIST AI Risk Management Framework (AI RMF 1.0). Such framework will include: (a) documented policies governing AI Model development, testing, deployment, monitoring, and retirement; (b) designated personnel responsible for AI governance oversight; (c) risk assessment processes for evaluating the potential harms and benefits of AI Services prior to deployment; (d) incident response procedures for AI-related failures, including notification timelines, root cause analysis, and remediation protocols; and (e) periodic review of AI governance policies at least annually to account for regulatory and technological developments.

13.2. AI Model Documentation. For each AI Model used to provide AI Services, RealCISO will maintain documentation describing: (a) the intended purpose and approved use cases; (b) known limitations, including categories of inputs for which the AI Model may produce unreliable outputs; (c) performance metrics, including accuracy benchmarks relevant to the stated use cases; (d) a summary of the types and sources of data used in training (without disclosing proprietary training datasets or trade secrets); (e) model versioning and material update history; and (f) the risk classification of the AI Model under applicable US state AI regulations. RealCISO will make a summary of such documentation available to Customer upon written request within thirty (30) days.

13.3. Automated Decision-Making Transparency.

13.3.1. Identification. RealCISO will clearly identify within the Services documentation and user interface which features constitute or support Automated Decisions as defined in Section 1A. RealCISO will maintain a current list of such features and make it available to Customer.

13.3.2. Human Oversight. For any AI Service feature that supports Automated Decisions, RealCISO will provide mechanisms enabling Customer to: (a) implement human review before acting on AI Outputs; (b) override or modify AI Outputs; (c) disable specific AI features if

Customer determines they are not appropriate for Customer's use case; and (d) configure the level of automation appropriate for Customer's risk tolerance and regulatory requirements.

13.3.3. Explainability. Upon Customer's reasonable request, RealCISO will provide a plain-language explanation of the principal factors contributing to a specific AI Output, to the extent technically feasible without disclosing trade secrets in the AI Model architecture. RealCISO will respond to such requests within fifteen (15) business days.

13.3.4. Consumer Notices. To the extent required by applicable US law (including the California Consumer Privacy Act Automated Decision-Making Technology regulations and the Colorado Artificial Intelligence Act), RealCISO will provide Customer with templates or tools enabling Customer to deliver required pre-use notices, opt-out mechanisms, and access rights disclosures to its end users regarding the use of AI Services.

13.4. Fairness and Bias.

13.4.1. Bias Testing. RealCISO will conduct bias and fairness testing of AI Models at least annually, and upon any material model update, using industry-recognized methodologies consistent with the NIST AI RMF. RealCISO will make a summary of bias testing results available to Customer upon written request, subject to the confidentiality obligations in Section 5.

13.4.2. Bias Reporting. Customer may report suspected bias or unfair outcomes in AI Outputs to RealCISO at the email address designated in the AI Acceptable Use Policy. RealCISO will acknowledge receipt within five (5) business days and will investigate such reports within thirty (30) days, providing Customer with a written summary of findings and any corrective actions taken or planned.

13.4.3. Non-Discrimination Commitment. RealCISO is committed to developing and deploying AI Services that do not unlawfully discriminate on the basis of race, color, religion, sex, national origin, age, disability, genetic information, or other characteristics protected by applicable law. RealCISO will take commercially reasonable steps to identify, measure, and mitigate potential algorithmic discrimination in AI Services, including through the bias testing described in Section 13.4.1 and by incorporating fairness considerations into AI Model design and training processes.

13.5. AI Model Updates and Change Management.

13.5.1. Material Changes. RealCISO will provide Customer with at least thirty (30) days' written notice before implementing any material change to an AI Model that is reasonably expected to significantly alter the nature, accuracy, or behavior of AI Outputs. For purposes of this section, a "material change" includes: (a) replacement of an AI Model with a different model; (b) significant retraining that changes the model's behavior on more than twenty percent (20%) of representative test cases; or (c) changes to the model architecture (e.g., switching foundation model providers).

13.5.2. Emergency Updates. Notwithstanding Section 13.5.1, RealCISO may implement emergency updates to AI Models without advance notice where necessary to address: (a) security vulnerabilities in AI Services; (b) regulatory non-compliance identified in AI Services; (c) the generation of harmful, dangerous, or discriminatory outputs; or (d) material performance degradation. RealCISO will notify Customer of any emergency update within five (5) business days and will provide a summary of the changes made and the reasons therefor.

13.5.3. Rollback Rights. For a period of thirty (30) days following any material AI Model update under Section 13.5.1, Customer may request that RealCISO revert to the prior version of the AI Model. RealCISO will use commercially reasonable efforts to accommodate such request,

subject to: (a) technical feasibility; (b) security considerations; and (c) the prior version's continued compliance with applicable law. If rollback is not feasible, RealCISO will promptly notify Customer and, at Customer's election, Customer may terminate the affected Order Form without penalty.

13.6. Regulatory Compliance.

13.6.1. Applicable AI Laws. RealCISO will use commercially reasonable efforts to ensure that the AI Services, as provided by RealCISO to Customer, comply with applicable US AI-specific laws and regulations, including but not limited to: (a) US state AI regulations applicable to the jurisdictions in which Customer is authorized to deploy the Services, including the Colorado Artificial Intelligence Act (SB 24-205), California Consumer Privacy Act Automated Decision-Making Technology regulations, and the Texas Responsible AI Governance Act; (b) the NIST AI Risk Management Framework (AI RMF 1.0) to the extent RealCISO represents compliance therewith.

13.6.2. Cooperation. RealCISO will reasonably cooperate with Customer in responding to regulatory inquiries, audits, complaints, or enforcement actions related to Customer's use of AI Services, including by providing documentation, technical information, and access to relevant personnel reasonably necessary for Customer to demonstrate compliance with applicable AI regulations. Such cooperation will be at RealCISO's expense to the extent the inquiry relates to RealCISO's obligations under this MSA, and at Customer's expense to the extent it relates to Customer's use of AI Services.

13.6.3. Regulatory Updates. RealCISO will monitor changes in applicable US AI laws and regulations that are reasonably likely to affect the AI Services and will: (a) update the AI Services as reasonably necessary to maintain compliance; (b) update this MSA in accordance with Section 12.8 (Amendments) as required by changes in applicable AI law; and (c) notify Customer of material regulatory developments that may affect Customer's use of AI Services within thirty (30) days of RealCISO becoming aware of such developments.

13.6.4. Recordkeeping. RealCISO will maintain records of AI governance activities, including AI Model documentation, bias and fairness testing results, incident reports, and change management logs, for a minimum of three (3) years or such longer period as required by applicable law. Such records will be made available to Customer or its auditor upon reasonable written request under Section 6.5.7 (AI Audit Rights).

13.6.5. International Compliance. The AI Services are currently designed and operated for use within the United States. If Customer intends to use AI Services in connection with data subjects, operations, or regulatory obligations outside the United States, the Parties will negotiate and execute an International AI Compliance Addendum addressing jurisdiction-specific requirements, including but not limited to the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), GDPR Article 22 (Automated Decision-Making), and other applicable international AI regulations, prior to such use. RealCISO reserves the right to restrict access to AI Services in jurisdictions where compliance requirements have not been addressed by an applicable addendum.