Data Processing Agreement

This Data Processing Agreement, including all its Schedules (the "DPA"), is entered into between Aikido and Customer and is incorporated into and forms part of the Aikido Master Subscription Agreement (MSA), as applicable (the "Agreement"), entered into by and between Customer and Aikido. This DPA governs the data processing service related to the Services as described by, and procured through, the Agreement. All capitalized terms used but not defined in this DPA shall have the meanings set forth in the Agreement. In the event of a conflict between the Agreement and the DPA, the terms of the DPA shall prevail as to the processing of Personal Data, subject to Articles 10.3 and 12.

The Schedules form an integral part of this DPA: Schedule 1 describes the processing of Personal Data for each Service, and Schedule 2 sets out the Technical and Organizational Measures.

1. SCOPE, ROLES AND DETAILS OF PROCESSING

1.1. **Scope and purpose.** For the purpose of this DPA, Aikido shall be Processor and Customer shall be Controller with respect to the Personal Data processed under the Agreement. This DPA is entered into in the context of the Agreement and governs all processing of Personal Data by Aikido on behalf of Customer in relation to the processing activities described in Schedule 1.

1.2. **Details of the Processing.** The subject-matter, nature and purpose of the processing, the types of Personal Data, the categories of Data Subjects, and the retention periods are set out in Schedule 1 for each Service. The sections of Schedule 1 apply only if Customer has requested the relevant Service under the Agreement.

1.3. **Duration.** This DPA takes effect at the start of the Subscription Term and remains in force for as long as the Agreement does. The processing of Personal Data shall only last for the duration of Customer's use of the Services, after which the Personal Data will be deleted in accordance with Article 8. The Agreement's termination and survival provisions, including Section 7.5 (Survival) of the Agreement, apply to this DPA.

1.4. **Customer responsibilities.** As Controller, Customer is responsible for (i) establishing a lawful basis for the processing of Personal Data under the Agreement and giving all notices and obtaining all consents and employee-representative approvals required under applicable law; (ii) ensuring that its instructions comply with the Data Protection Laws; and (iii) ensuring that the Customer Content it submits or makes available to the Services complies with the Agreement and this DPA.

2. DOCUMENTED INSTRUCTIONS

2.1. **Processing instructions.** The Agreement and this DPA together constitute Customer's instructions for the processing of Personal Data. Aikido confirms that it shall only Process Personal Data on Customer's behalf and for no other purpose. Aikido shall inform Customer if, in its opinion, an instruction infringes the applicable Data Protection Laws, and may suspend the relevant processing until Customer confirms or modifies the instruction.

2.2. **Processing required by law.** Aikido shall only Process or disclose Personal Data to a third party on Customer's behalf (i) under Customer's written instructions given under the Agreement or this DPA, or (ii) if required by EU or member state law (or, for the UK GDPR, UK law), in which case Aikido shall notify Customer of the legal requirement, the Personal Data concerned, and the processing required, to the extent legally permitted.

3. CONFIDENTIALITY

3.1. **Confidentiality obligations.** The confidentiality provisions of the Agreement remain in full force and effect and are incorporated by reference into this DPA and apply to all Personal Data and other information Aikido becomes aware of in connection with the Services. Personal Data is treated as Confidential Information irrespective of marking, and Aikido's duty of confidentiality in respect of Personal Data continues for as long as Aikido holds it, notwithstanding any shorter period in the Agreement.

3.2. **Confidentiality of personnel and Sub-Processors.** Aikido shall ensure that all employees, contractors, agents, representatives, and Sub-Processors who may access Personal Data are bound by confidentiality obligations at least as protective as those applicable to Aikido's own processing of that data and shall only make Personal Data available to personnel directly involved in performing the Agreement, on a strict need-to-know basis.

3.3. **Disclosure to Sub-Processors.** To the extent necessary to implement this DPA, Aikido may disclose Confidential Information to its Sub-Processors as may be reasonably necessary, if Aikido ensures such Sub-Processors are bound by a similar duty of confidentiality.

4. SECURITY OF PROCESSING

4.1. **Security.** Aikido will maintain the technical and organizational security measures required by Section 3.2 of the Agreement, which are further detailed in Schedule 2 to this DPA. Aikido may update or modify them from time to time, provided such updates do not result in a material reduction of the protection provided for Personal Data.

5. SUB-PROCESSORS

5.1. **Authorization.** Customer grants Aikido the authorization to engage Sub-Processors to process Personal Data. Aikido shall maintain an up-to-date list of Sub-Processors at https://trustcenter.aikido.dev/subprocessors and as set forth in Schedule 1.

5.2. **Notice and objection.** Aikido shall give Customer at least thirty (30) days' written notice before adding or replacing a Sub-Processor. If Customer does not object in writing, with reasons, within thirty (30) days of that notice, Customer is deemed to have consented. If Customer objects within that period, the Parties shall discuss Customer's concerns in good faith to reach a commercially reasonable resolution.

5.3. **Flow-down and responsibility.** Aikido shall ensure each Sub-Processor is appointed under a written agreement conferring materially the same obligations with respect to Personal Data as this DPA and shall be responsible for ensuring each Sub-Processor complies with those obligations.

6. DATA SUBJECT RIGHTS

6.1. **Assistance.** Aikido shall, upon Customer's written instruction, provide reasonable assistance to Customer in responding without undue delay to a request from a Data Subject seeking to exercise its rights under the applicable Data Protection Laws, including requests regarding access, rectification, erasure, or restriction of processing. Customer shall inform Aikido of any such request with which Aikido must comply and shall provide Aikido the information necessary to do so.

6.2. **Requests received by Aikido.** If Aikido receives a request from a Data Subject or Consumer relating to Personal Data Processed on behalf of Customer, Aikido shall refer that person to Customer and shall not respond substantively except on Customer's instruction or as required by law.

7. ASSISTANCE WITH CUSTOMER'S COMPLIANCE OBLIGATIONS

7.1. **Compliance assistance.** Aikido shall provide Customer with reasonable assistance to help Customer meet its own obligations under the applicable Data Protection Laws, including by (i) implementing appropriate technical and organizational measures as referenced in Schedule 2, (ii) responding to Data Subject rights requests under Article 6, and (iii) making available to Customer, upon Customer's reasonable request, information in Aikido's possession necessary to demonstrate Aikido's compliance with this DPA. Aikido shall notify Customer if it determines that it can no longer meet its obligations under the applicable Data Protection Laws, in which case Customer may direct Aikido to take reasonable and appropriate steps to remediate.

7.2. **Personal Data Breach.** Aikido shall notify a Personal Data Breach to Customer in writing, without undue delay upon becoming aware of it, and provide Customer all reasonably necessary assistance and information, including, to the extent known to Aikido, the nature of the breach, the categories and approximate number of Data Subjects and Personal Data records concerned, the likely consequences, and the measures taken or proposed to address it.

7.3. **Impact assessments and consultation.** Aikido shall, where possible, assist Customer with preparing a data protection impact assessment, any required prior consultation with a supervisory authority, and any assessment, inquiry, notice, or investigation under the GDPR or UK GDPR.

8. RETURN OR DELETION

8.1. **Return or deletion.** Upon termination or expiration of the Agreement, Aikido shall delete Personal Data within the period set out in Section 7.4.4 of the Agreement. At Customer's written request made upon termination or expiration of the Agreement, Aikido shall, within thirty (30) days of that request: (i) return a complete copy of all Personal Data to Customer by secure file transfer, in the format Customer specifies, and securely erase all other copies held by Aikido or any Sub-Processor; or (ii) securely erase all copies of Customer's Personal Data held by Aikido or any Sub-Processor. Without prejudice to the foregoing, Aikido has no control over any sharing of information that Customer exclusively configures or directs through its use of the Services; only Customer can stop such sharing, and Customer remains solely responsible for it.

8.2. **Retention required by law.** Aikido may retain Personal Data beyond that point only as long as required by applicable law, provided it keeps that information confidential and continues to protect it in accordance with this DPA.

9. INFORMATION AND AUDITS

9.1. **Audit.** Customer may carry out a documentary audit, itself or through third-party auditors, to verify Aikido's compliance with this DPA and the applicable Data Protection Laws, but only where less intrusive measures (such as the certifications and reports referred to in Article 9.2) do not suffice to verify such compliance, and on at least thirty (30) business days' prior written notice to Aikido. Such audit may not be carried out more than once per calendar year, unless applicable Data Protection Laws require otherwise, there are strong indications of suspected non-compliance, or the audit follows a Personal Data Breach. Nothing in this Article limits any audit or inspection that a Supervisory Authority is entitled

to carry out under applicable Data Protection Laws. Where a Supervisory Authority or applicable Data Protection Laws require an on-site audit, Aikido will permit and cooperate with it on reasonable prior notice, subject to Article 9.3.

9.2. **Certifications and reports.** Before or instead of an audit under Article 9.1, Aikido may provide current ISO 27001 certificates, SOC 2 reports, summary audit reports, or other relevant documentation to address the request, and Customer agrees to review these in good faith before requesting a further audit.

9.3. **Third-party auditors and costs.** If Customer wishes to use third-party auditors, Customer shall give Aikido at least thirty (30) business days' written notice before the audit, naming the auditor, who must have proven data protection expertise and must not be a competitor of Aikido. Aikido may refuse a specific auditor and request another, if it gives Customer written reasons at least seven (7) business days before the audit's planned start. The cost of the audit will be borne by Customer, unless the audit shows that Aikido or any of its Sub-Processors is materially infringing this DPA or the applicable Data Protection Laws. Customer shall ensure that its employees or appointed third-party auditors are bound by confidentiality obligations, whether contractual or statutory, and the audit shall be carried out in a manner that minimizes disruption to Aikido's business.

10. INTERNATIONAL DATA TRANSFERS

10.1. **Scope of this Article.** This Article applies only to the extent Customer and the Personal Data Aikido Processes for Customer fall within the scope of the GDPR, UK GDPR, or the Swiss Federal Act on Data Protection, and only to transfers of that Personal Data to a third country or international organization.

10.2. **Transfers.** In providing the Services, Aikido may transfer Personal Data to third countries. In such case, Aikido will ensure that each such transfer complies with the GDPR, UK GDPR, or the Swiss Federal Act on Data Protection, as applicable, has an appropriate legal basis and, where applicable, has adopted appropriate safeguards. Such appropriate safeguards may be provided by (i) binding corporate rules accepted by the competent Supervisory Authority, (ii) standard data protection clauses adopted by the European Commission or by a supervisory authority and approved by the European Commission, or (iii) an approved code of conduct under Article 40 GDPR or an approved certification mechanism under Article 42 GDPR.

10.3. **Standard Contractual Clauses.** Where Standard Contractual Clauses are required for a transfer of Personal Data under this DPA, they are incorporated by reference, with Aikido as data exporter and the relevant Sub-Processor as data importer (Module Three), Annex I completed by Schedule 1, Annex II completed by Schedule 2, Clause 9(a) Option 2 applying with the notice period in Article 5.2, and Clauses 17 and 18 governed by the law and courts of Belgium. Where the UK GDPR or the Swiss Federal Act on Data Protection applies, the UK International Data Transfer Addendum or the equivalent Swiss amendments are likewise incorporated. In the event of a conflict, the Standard Contractual Clauses prevail to the extent required by law.

11. U.S. PRIVACY LAWS

11.1. **Application and roles.** This Article applies in addition to the other provisions of this DPA, and only to the extent Aikido processes Personal Data that is subject to U.S. Privacy Laws. If it conflicts with another provision of this DPA with respect to that Personal Data, this Article prevails. Customer is the Controller (or "Business") and appoints Aikido as its Processor (or "Service Provider" or "Contractor") to process that Personal Data solely for the limited and specific purposes of providing the Services described in Schedule 1 (the "Business Purposes").

11.2. **Restrictions on Processing.** Aikido will Process Personal Data as instructed in the Agreement. Except as the U.S. Privacy Laws expressly permit, Aikido may not (i) sell or share Personal Data; (ii) retain, use, or disclose it for any purpose other than the Business Purposes; (iii) retain, use, or disclose it outside the Parties' direct business relationship; or (iv) combine it with personal information from sources other than Customer. Customer discloses Personal Data to Aikido only for the Business Purposes, and no monetary or other valuable consideration is exchanged for it. To the extent Aikido acts as a Contractor, Aikido certifies that it understands and will comply with these restrictions.

11.3. **Compliance and oversight**. Aikido shall comply with the U.S. Privacy Laws applicable to it as a Processor, shall provide the same level of privacy protection as those laws require of Customer, and shall notify Customer in writing within five (5) business days if it determines that it can no longer meet its obligations under them. Upon written notice, Customer may take reasonable and appropriate steps to ensure that Aikido uses the Personal Data consistently with Customer's obligations under the U.S. Privacy Laws and to stop and remediate any unauthorized use.

11.4. **Consumer requests**. Article 6 applies to requests from Consumers. Aikido need not delete Personal Data to comply with a Consumer request from Customer if the U.S. Privacy Laws specifically permit retaining it, provided Aikido uses the retained information only for the purpose the exception allows.

11.5. **Deidentified data**. To the extent any Personal Data is deidentified by Aikido or Customer, Aikido shall take reasonable measures to ensure the deidentified data cannot be associated with a Consumer or household and shall not attempt to reidentify it.

11.6. **Controller/Processor-model state laws**. To the extent Personal Data is subject to a U.S. state privacy law that uses “Controller” and “Processor” terminology (including the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act, each as amended), Aikido shall Process that Personal Data only under Customer’s documented instructions as set out in Article 2, and the obligations set out in Article 4 (Security of Processing), Article 5.3 (Flow-down and responsibility), Article 6 (Data Subject Rights), Article 7.2 (Personal Data Breach), and Article 7.3 (Impact assessments and consultation) apply to satisfy the corresponding Processor obligations under those laws.

11.7. **Breach notice timing**. Aikido shall provide the notice required by Article 7.2 with the promptness necessary to allow Customer to meet any shorter notification deadlines imposed on Customer by applicable U.S. Privacy Laws.

12. LIABILITY

12.1. **Liability cap.** Aikido’s liability under this DPA is subject to the limitations and exclusions of liability set out in the Agreement, and nothing in this DPA increases Aikido’s liability beyond that.

13. CHANGES TO THE DPA

13.1. **Modifications.** Aikido may modify this DPA in response to (i) changes in Data Protection Laws; (ii) a merger, acquisition, reorganization, or similar event; or (iii) new or materially changed Services. Aikido will make modifications by posting a revised DPA at https://www.aikido.dev/ or by otherwise notifying Customer. Modifications required by a change in Data Protection Laws take effect thirty (30) days after posting, notwithstanding the Updates to the MSA and DPA section of the Agreement; other modifications apply in accordance with the Updates to the MSA and DPA section of the Agreement. No modification may result in a material reduction of the protection provided for Personal Data, and a DPA signed by both Parties may be amended only in writing signed by both Parties.

14. GOVERNING LAW, VENUE AND DISPUTES

14.1. **Governing law.** Governing law, venue, and dispute resolution for this DPA follow the Agreement, including its good-faith negotiation requirement before court proceedings. Either Party may still seek interim or injunctive relief from a competent court to protect its rights.

15. DEFINITIONS AND INTERPRETATION

15.1. **Interpretation.** The terms “Controller”, “Personal Data”, “Processor” (which includes “Service Provider” or “Contractor” under U.S. Privacy Laws, where applicable), “Processing”, “Process”, “Data Subject”, “Sub-Processor” and “Supervisory Authority” have the same meaning as in the applicable Data Protection Laws. Singular includes plural and vice versa.

15.2. **Structure.** Where this DPA refers to a provision of the GDPR, it also refers to the equivalent provision of the UK GDPR where the UK GDPR applies. Not all provisions of this DPA will apply in every situation; this depends on the applicable Data Protection Laws, the Services ordered by Customer, and other relevant circumstances.

Consumer	A natural person. Where applicable, Consumer shall be interpreted consistent with the same or similar term under the U.S. Privacy Laws.
Data Protection Laws	The national, federal, state, provincial, or local privacy, cybersecurity, and data protection regulations, together with any implementing or supplemental rules and implementing acts, applicable to Aikido’s processing of Personal Data as necessary to provide the Services, but in any case, limited to the following data protection regulations: (a) EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“GDPR”); (b) the UK General Data Protection Regulation, as it forms part of the law of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018, as further amended by the Data Protection Act 2018 (“UK GDPR”); (c) U.S. Privacy Laws; and (d) any other data protection or privacy law of any jurisdiction (including the Swiss Federal Act on Data Protection) to the extent it applies to Aikido’s processing of Personal Data as a Processor under the Agreement, in which case Aikido’s obligations under this DPA apply to

	the extent they correspond to the obligations that law imposes on a Processor and, where that law requires additional terms, the Parties will agree them in good faith.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
Standard Contractual Clauses	The standard contractual clauses for the transfer of personal data to third countries adopted by European Commission Implementing Decision (EU) 2021/914 and, where relevant, the International Data Transfer Addendum to those clauses or the International Data Transfer Agreement issued under section 119A of the UK Data Protection Act 2018, each as amended or replaced from time to time.
Technical and Organizational Measures	The technical and organizational measures taken by Aikido pursuant to Article 32 GDPR, as further detailed in Schedule 2.
U.S. Privacy Laws	All applicable U.S. federal and state privacy laws and their implementing regulations, as amended or superseded, that apply generally to the processing of individuals' personal information, and not laws limited to specific industry sectors (e.g. financial institutions), demographics (e.g. children), or data types (e.g. health or biometric information), to the extent applicable to Aikido's processing of Personal Data under the Agreement. U.S. Privacy Laws include the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations, but exclude the Health Insurance Portability and Accountability Act of 1996.

Schedule 1: Data Processing Details

The Processing activities described in this Schedule depend on the Services Aikido provides to Customer under the Agreement. Section 1 applies to processing as part of Aikido Security, and Section 2 applies to processing as part of Noon. A subsection applies only if Customer has requested the relevant Service under the Agreement.

Section 1: Processing as part of Aikido Security

Services covered	Aikido Security (including, where procured, AI Pentest, Device Protection)
Categories of Data Subjects	Developers and other employees of Customer who are users of Aikido's Services or who otherwise contribute to Customer's code base, as well as any other individuals referenced or identifiable in Customer's source code or other Customer Content submitted to the Services (for example, in commit metadata, code comments, or file contents). *Leaked credential monitoring (optional):* any individuals with information (such as credentials) that can be used to identify and exploit vulnerabilities in Customer's IT systems, including Customer's employees and external advisors.
Categories of Personal Data	First and last name, employer, title, and position; email addresses; user ID on source code repositories and other services integrated with Aikido by Customer's users; connection and/or localization data; support correspondence and usage logs. *Device Protection (optional)*: device identifiers and hostnames; operating system information; username and email address; installed packages, extensions, plug-ins, and AI tools (including MCP servers and models); package installation and blocked-install events; domains contacted and blocked by the device firewall. *AI Pentest (optional)*: Personal Data stored on Customer's in-scope systems subject to an AI Pentest and, where Customer authorizes Credential-Based Testing under the AI Penetration Testing Addendum, usernames, email addresses, passwords, and other data accessible upon successful authentication. *Leaked credential monitoring (optional):* first and last name, email addresses, user ID, login credentials, IP addresses, and other data enabling the identification or exploitation of vulnerabilities in Customer's IT systems identified on the Dark Web or other publicly available resources.
Sensitive Personal Data	None, except that Personal Data accessed in the course of an AI Pentest may incidentally include Sensitive Personal Data
Frequency of the Personal Data transfer	Ongoing and continuous throughout the provision of the Services (for example on each commit, pull request, or scan request, or on the schedule configured by Customer). *AI Pentest (optional)*: occasionally, when an AI Pentest is planned and executed, or on every release for continuous pentesting.
Nature of the Processing	Automated scanning and analysis of Customer's source code, dependencies, cloud configurations, applications, and devices to identify and report security findings, including through read-only cloud connections, test requests to Customer-designated targets, and a local agent that blocks attacks or malicious packages. Where AI-assisted features are enabled, relevant code excerpts are submitted to AI model providers acting as Sub-Processors to generate findings, explanations, or proposed fixes; Aikido does not use Customer Content to train AI models, as provided in the Agreement. Any processing of Personal Data is incidental to these operations and occurs only to the extent Personal Data is present within the source code, configurations, or other data scanned.
Retention period	As long as required for the provision of the relevant Service, however, no longer than the Subscription Term plus the deletion period in Article 8 of this DPA.

Transfers to Sub-Processors	See https://trustcenter.aikido.dev/subprocessors.

Section 2: Processing as part of Noon

This section applies to Noon, Aikido's human-risk-management services. The processing described below depends on the modules Customer uses and the permissions Customer (or its administrator) grants.

Services covered	• Email Protection: scanning of inbound email in Customer's Google Workspace or Microsoft 365 tenant to detect phishing, business email compromise, credential harvesting, and malware (including by checking sender authentication, sender identity claims, link destinations and behavior, and attachments), and triage of emails reported by employees. • AI governance (Shadow AI visibility), breach monitoring, people and directory management, reports, and integrations. • Device Protection and Endpoint Agent: protection of devices, including the optional EDR Mode where available. • Phishing simulations & training: simulated phishing by email, SMS, chat, voice, and deepfake, adaptive security-awareness training, including in Slack, Teams, or Google Chat.
Categories of Data Subjects	Monitored Individuals, as defined in the Agreement.
Categories of Personal Data	• Email Protection: email content and metadata (headers, body, attachments, sender/recipient, subject, dates, authentication and classification results); reported emails; mailbox settings; where write access is granted, labels, categories, and folder actions. • AI governance: AI tools, models, and AI SaaS services used by Monitored Individuals, derived from device and email data and, where Customer enables cloud analysis, the AI prompt content sent to the cloud for analysis. • Device Protection and Endpoint Agent: device identifiers, OS and agent version, user/group, posture, installed software, and block events; if EDR Mode is enabled, process, network, and persistence events relating to individuals. • Breach monitoring: corporate email addresses of Monitored Individuals and the breach exposure results returned for them, such as the breach concerned and the types of data exposed. • Simulations & training: recipient identity, delivery/click/response data, contact identifiers, and (for voice/deepfake) recordings and transcripts; course assignments, progress, and quiz responses.
Sensitive Personal Data	May incidentally include Sensitive Personal Data or special categories of data, and other sensitive information such as secrets or payment card data, for example where an email, a simulation response, a recording, or a prompt submitted for cloud analysis references them. Aikido has no control over or visibility into what Monitored Individuals or third parties include in such communications before they are processed. Customer remains responsible for the lawfulness of monitoring Monitored Individuals, including any employee-representative approval.
Frequency of the Personal Data transfer	Ongoing and continuous for email scanning (near real-time after an initial scan of existing mail), the Endpoint Agent, and AI and SaaS usage detection; one-time for a one-time mailbox read; and per campaign for simulations and training.
Nature of the processing	• Email protection: connecting a mailbox is read-only; Aikido will request Customer's permission before moving or modifying any message, and, unless Customer enables automation, actions on flagged mail require Customer's approval. Only emails flagged as

	suspicious or malicious (for example spam, malware, or phishing) are stored in Noon for verification; other emails are scanned and deleted immediately after analysis without persistent storage of the message, although the resulting verdict and aggregate counts are retained, and messages pending a decision remain available until reviewed. Where write access is granted, modification of mailbox items, including moving a flagged message to or from spam, threats, trash, or the inbox at Customer's direction. • AI Governance: automated inventory of AI tools, models, providers, and MCP servers in use, built from device and email data (such as device telemetry and email headers and sender domains) rather than self-reported by Monitored Individuals; display of the models, providers, MCP servers, and tools in use and the devices running them; and, where Customer elects to allow or block a tool, enforcement of that setting. By default, AI prompts and conversation content remain on the device, are not transmitted to Noon, and cannot be seen by Customer's administrators. Where Customer enables cloud analysis, the prompt data sent to the cloud for analysis is processed by Aikido and its Sub-Processors and is visible to Customer's administrators in Noon. • Device Protection and Endpoint Agent: enforcement of allow/block decisions locally on the device, using allowlists, blocklists, malware signatures, and policy rules (including an optional firewall policy) synced from Noon. Only the resulting outcomes are stored by Noon: allowed, blocked, and flagged install attempts; a daily list of installed packages; and a short heartbeat confirming the device is online. For a blocked package, Customer can see its version, origin, and the reason it was blocked; for a blocked site, only the domain is visible. Other than where Customer enables EDR Mode, in which case process, network, and persistence events are also transmitted to Noon, file contents, browsing activity, page content, and (unless Customer enables cloud analysis) AI prompts are not transmitted and remain on the device. • Simulations & training: delivery of simulated phishing messages by email, SMS, chat, voice, and deepfake, as the case may be through Sub-Processors, using write access to place the message directly in the mailbox; recording of each Monitored Individual's response (opened, compromised, or reported) and delivery of a lesson specific to that message if the individual is caught, with each person able to see only their own result; delivery of training content and recording of course progress and completion; breach look-ups against breach-data providers; and storage and display of aggregate results (such as compromise and report rates) and reports to Customer. Results are not visible to other Monitored Individuals. Aikido does not use Customer Content to train AI models, as provided in the Agreement.
Purpose(s) of the Personal Data transfer	Reducing Customer's human-factor security risk by detecting phishing and other threats, simulating attacks, training personnel, protecting devices, and giving Customer visibility into exposure and AI and SaaS usage.
Retention period	Email Protection: emails assessed as safe are deleted immediately after analysis (only the verdict and aggregate counts are retained). Emails flagged as suspicious or malicious are retained for the Subscription Term and purged within 200 days after termination of the Agreement, or earlier at Customer's written request, in accordance with Article 8.1 and the Agreement. All other Noon data: as specified in Article 8.1 of the DPA.
Transfers to Sub-Processors	See https://trustcenter.aikido.dev/subprocessors

Schedule 2: Technical and Organizational Measures

The Technical and Organizational Measures are the measures taken by Aikido, as further detailed in this Schedule 2. Aikido may update or modify them from time to time, provided such updates do not result in a material reduction of the protection provided for Personal Data.

Accountability and Certification

Aikido Security BV follows internal governance protocols to ensure compliance with data protection regulations.

External certifications, such as ISO/IEC 27001 and SOC 2, are maintained to demonstrate compliance with security standards.

What follows are a selection of relevant policies describing technical and organizational measures undertaken.

Infrastructure security

Unique production database authentication enforced

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.

Encryption key access restricted

The company restricts privileged access to encryption keys to authorized users with a business need.

Access control procedures established

The company's access control policy documents the requirements for the following access control functions:

* adding new users;

* modifying users; and/or

* removing an existing user's access.

Production database access restricted

The company restricts privileged access to databases to authorized users with a business need.

Firewall access restricted

The company restricts privileged access to the firewall to authorized users with a business need

Production OS access restricted

The company restricts privileged access to the operating system to authorized users with a business need

Production network access restricted

The company restricts privileged access to the production network to authorized users with a business need

Access revoked upon termination

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs

Unique network system authentication enforced

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Shell (SSH) keys

Remote access MFA enforced

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method

Remote access encrypted enforced

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

Intrusion detection system utilized

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

Log management utilized

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives

Network segmentation implemented

The company’s network is segmented to prevent unauthorized access to customer data

Network firewalls reviewed

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

Network firewalls utilized

The company uses firewalls and configures them to prevent unauthorized access.

Network and system hardening standards maintained

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

Organizational security

Asset disposal procedures utilized

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

Portable media encrypted

The company encrypts portable and removable media devices when used

Anti-malware technology utilized

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

Employee background checks performed

The company performs background checks on new employees

Code of Conduct acknowledged by contractors

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

Code of Conduct acknowledged by employees and enforced

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

Confidentiality Agreement acknowledged by contractors

The company requires contractors to sign a confidentiality agreement at the time of engagement.

Confidentiality Agreement acknowledged by employees

The company requires employees to sign a confidentiality agreement during onboarding.

Performance evaluations conducted

The company managers are required to complete performance evaluations for direct reports at least annually.

Password policy enforced

The company requires passwords for in-scope system components to be configured according to the company's policy.

MDM system utilized

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

Visitor procedures enforced

The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.

Product security

Data encryption utilized

The company's datastores housing sensitive customer data are encrypted at rest.

Control self-assessments conducted

The company performs control self-assessment at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.

Penetration testing performed

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs

Data transmission encrypted

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

Vulnerability and system monitoring procedures established

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

* vulnerability management;

* system monitoring.

Internal security procedures

Continuity and Disaster Recovery plans established

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel

Continuity and disaster recovery plans tested

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

Cybersecurity insurance maintained

The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions

Configuration management system established

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

Development lifecycle established

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements

Whistleblower policy established

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns

Board oversight briefings conducted

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed

Board charter documented

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

Board expertise developed

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed

Board meetings conducted

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

Backup processes established

The company's data backup policy documents requirements for backup and recovery of customer data

System changes externally communicated

The company notifies customers of critical system changes that may affect their processing.

Management roles and responsibilities defined

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

Organization structure documented

The company maintains an organizational chart that describes the organizational structure and reporting lines.

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

Security policies established and reviewed

The company's information security policies and procedures are documented and reviewed at least annually.

Support system available

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

System changes communicated

The company communicates system changes to authorized internal users

Access reviews conducted

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

Access requests required

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned

Incident response plan tested

The company tests their incident response plan at least annually.

Incident response policies established

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

Physical access processes established

The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

Data center access reviewed

The company reviews access to the data centers at least annually

Company commitments externally communicated

The company's security commitments are communicated to customers in Master Subscription Agreements (MSA) or Terms of Service (TOS)

External support resources available

The company provides guidelines and technical support resources relating to system operations to customers

Service description communicated

The company provides a description of its products and services to internal and external users.

Risk assessment objectives specified

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

Risks assessments performed

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

Risk management program established

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

Third-party agreements established

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

Vendor management program established

The company has a vendor management program in place. Components of this program include:

* critical third-party vendor inventory;

* vendor's security and privacy requirements; and

* review of critical third-party vendors at least annually.

Data and privacy

Data retention procedures established

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

Customer data deleted upon leaving

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

Data classification policy established

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.