RETACH

MUTUAL NON-DISCLOSURE AGREEMENT

Under the RETACH vCISO Master Engagement Framework

Document Control	
Status	Version 1.0 template
Parties	RETACH Digital Ltd and [Client legal name]
Applies to	vCISO Fixed-Scope Engagement and any SOW under the Master Engagement Framework
Classification	Template — completed and signed for each client
Governing law	Republic of Kenya
Related documents	Master Engagement Framework (v1.0) · Scope of Services / SOW template · Schedule 1 (Personal Data Processing Details)

Parties and Background

This Mutual Non-Disclosure Agreement (the "Agreement") is made on [Effective Date] between:

(1) RETACH Digital Ltd, a private limited company incorporated in Kenya under the Companies Act, 2015 (Certificate No. PVT-WQ12RMY5), whose postal address is P.O. Box 26518-00100, Nairobi ("RETACH"); and

(2) [CLIENT LEGAL NAME], [registration number], whose address is [address] (the "Client").

Each is a "Party" and together the "Parties".

Background. The Parties intend to enter into a Master Engagement Framework (the "Framework") under which RETACH provides Virtual CISO (vCISO) services, with each engagement governed by its own Scope of Services / Statement of Work ("SOW"). In doing so each Party may disclose confidential information to the other, and RETACH may gain access to the Client's systems, security information and personal data. The Parties wish to protect that information on the terms below.

1. Definitions

1.1 "Confidential Information" means all information, in any form, that one Party or its Representatives (the "Discloser") discloses or makes available to the other Party (the "Recipient") in connection with the Purpose, that is marked or identified as confidential or that a reasonable person would understand to be confidential from its nature or the circumstances of disclosure. It includes Security Information, Personal Data, business and financial information, and (for RETACH) the RETACH Methodology.

1.2 "Security Information" means information about the security posture of a Party, including network diagrams, architectures, asset and identity inventories, system configurations, credentials, keys and tokens, logs, vulnerability, audit and testing findings, risk registers, incident details, and security policies and controls.

1.3 "Personal Data" has the meaning given in the Data Protection Act, 2019 (Kenya) (the "DPA"), and "controller", "processor", "data subject" and "personal data breach" have the meanings given in the DPA.

1.4 "Purpose" means evaluating, negotiating, entering into and performing the Framework and any SOW.

1.5 "Representatives" means a Party's directors, officers and employees, and its professional advisers (such as lawyers, auditors and insurers), who need to know Confidential Information for the Purpose. Subcontractors and associates are Representatives only with the Discloser's prior written consent, or if the SOW names them as pre-approved.

1.6 "RETACH Methodology" means the S.I.N.S. Framework, the CRQ Engine, RETACH's scoring models, templates, tools and other pre-existing intellectual property of RETACH, as described in the Framework.

2. Confidentiality Obligations

2.1 The Recipient shall:

(a) use Confidential Information only for the Purpose;

(b) keep it confidential and not disclose it to anyone except its Representatives under clause 2.2 or as permitted by clause 4;

(c) protect it with at least the care it uses for its own confidential information, and never less than reasonable care, including appropriate technical and organisational measures;

(d) make copies only as needed for the Purpose; and

(e) notify the Discloser promptly, and in any event within 48 hours (or, for a personal data breach affecting the Client's Personal Data, as clause 6.5 requires), on becoming aware of any unauthorised access, use or disclosure, and cooperate to contain and remedy it.

2.2 The Recipient may disclose Confidential Information to a Representative only if the Representative needs it for the Purpose and is bound by written or professional duties of confidentiality no less protective than this Agreement. The Recipient is responsible for any breach of this Agreement by its Representatives.

2.3 The Recipient shall not reverse engineer, decompile or attempt to re-identify any anonymised or pseudonymised information, except as an SOW authorises.

3. Exclusions

3.1 Clause 2 does not apply to information that the Recipient can show: (a) is or becomes public other than through breach of this Agreement; (b) was lawfully known to it, free of any duty of confidence, before disclosure; (c) is lawfully received from a third party free of any duty of confidence; or (d) is independently developed without use of the Confidential Information.

3.2 Clause 3.1 does not apply to Personal Data or to credentials, keys and tokens, which remain subject to clauses 2, 5 and 6.

4. Compelled Disclosure

4.1 If the Recipient is required by law, court order or a competent regulator (including the Data Commissioner) to disclose Confidential Information, it shall, where lawful, give the Discloser prompt prior written notice, disclose only the minimum required, and cooperate with any effort to obtain protective treatment.

4.2 Nothing in this Agreement prevents a Party from making a report to a competent authority that the law requires, including a personal data breach notification.

5. Security Information and Access

5.1 **Authorised access only.** Disclosure of Security Information, or the grant of access to a system, does not authorise RETACH to access, scan or test any system beyond what an SOW or a separate written authorisation signed by an authorised Client representative expressly permits. RETACH shall not perform intrusive activity (including exploitation, credential attacks or denial-of-service testing) unless the SOW expressly authorises it, and shall keep to the systems, methods and time windows authorised. The Client

confirms that it owns, or has the system owner's written authority to permit, access to each system in scope.

5.2 **Credentials.** Credentials and keys shall be exchanged only through a secure channel agreed in writing (not ordinary email), be individual and time-limited where practicable, follow least privilege, and be revoked or rotated when the work ends.

5.3 **Storage.** RETACH shall keep the Client's Security Information encrypted at rest, in access-controlled repositories that are logically separated from other clients' data, and shall not store it on personal devices or unmanaged accounts.

5.4 **Findings.** Vulnerability, audit, testing and risk findings about the Client's environment are the Client's Confidential Information. RETACH shall not disclose them to any third party, including any vendor or OEM partner, without the Client's prior written consent.

5.5 **Reporting vulnerabilities.** RETACH shall report to the Client's designated contact, promptly and in any event within 24 hours for a finding rated critical under the SOW, any vulnerability or exposure it discovers. Neither Party shall disclose it publicly.

5.6 **Vendors and OEMs.** RETACH shall share the Client's identity with an OEM, vendor or distributor only to the extent needed to quote, register or supply products the Client has asked about or ordered, and only after the Client consents (a signed quote or order counts as consent). RETACH shall not share any other Client information with them, and shall disclose to the Client in writing any commercial interest it holds in a product it recommends, as set out in the Framework.

6. Personal Data (Data Protection Act, 2019)

6.1 **Roles.** For Personal Data of the Client's data subjects that RETACH accesses or processes in performing the services, the Client is the data controller and RETACH is the data processor. Each Party is a controller of the business contact details of the other's personnel.

6.2 **Instructions.** RETACH shall process such Personal Data only on the Client's documented instructions, being this Agreement, the SOW and any further written instruction. RETACH acknowledges that under the DPA a processor that processes Personal Data other than as instructed may be treated as a controller of that processing.

6.3 **Minimisation.** The Client shall give RETACH access to Personal Data only where necessary for the services. RETACH shall avoid collecting or copying Personal Data, shall prefer redacted, sampled or pseudonymised evidence, and shall not remove Personal Data from the Client's environment unless the SOW requires it.

6.4 **Security.** RETACH shall implement appropriate technical and organisational measures to protect Personal Data, including encryption, access control, logging and personnel confidentiality, in line with section 41 of the DPA.

6.5 **Breach notification.** RETACH shall give the Client initial notice without undue delay, and in any event within 24 hours, after becoming aware of a personal data breach affecting the Client's Personal Data, and shall follow with further details as they become known, so that the Client can meet its own duties. The Client is responsible for notifying the Data Commissioner and the affected data subjects as section 43 of the DPA requires, and RETACH shall assist.

6.6 **Sub-processors.** RETACH shall not engage a sub-processor for the Client's Personal Data without the Client's prior written consent, and shall bind any approved sub-

processor to equivalent obligations. Products the Client buys are supplied under the OEM's own terms with the Client, and the OEM is not RETACH's sub-processor unless the SOW says so.

6.7 **Transfers outside Kenya.** RETACH shall not transfer the Client's Personal Data outside Kenya, and shall not use a service that processes it outside Kenya, unless the SOW or the Schedule identifies it in advance, the Client consents in writing, and the transfer complies with Part VI of the DPA (sections 48 to 50).

6.8 **Data subject requests and assistance.** RETACH shall forward any data subject request to the Client within 5 business days and shall give reasonable assistance with data subject rights, data protection impact assessments and consultation with the Data Commissioner.

6.9 **Compliance information.** RETACH shall provide the information reasonably needed to show compliance with this clause and allow one audit a year on reasonable notice, at the Client's cost.

6.10 **Registration.** Each Party confirms that it holds any registration with the Data Commissioner that the DPA requires for its role, or that it qualifies for an exemption.

6.11 **Precedence.** This clause prevails over any inconsistent term for Personal Data. If an SOW involves large-scale or sensitive Personal Data, the Parties shall first agree a separate data processing agreement.

7. Ownership and No Obligation

7.1 Confidential Information remains the property of the Discloser. No licence or other right is granted, except that the Client receives the licence to deliverables described in the Framework.

7.2 Confidential Information is provided as is, without warranty of accuracy or completeness, except as the SOW states. Neither Party is obliged to disclose information or to enter into the Framework or any SOW.

7.3 This Agreement creates no partnership or exclusivity. RETACH may serve other clients, including the Client's competitors, provided it does not use or disclose the Client's Confidential Information.

7.4 RETACH may use anonymised, aggregated and non-attributable data derived from the Client's environment (for example, in the Kenya Digital Risk Index) only if the Client has agreed in writing, and only if the Client and its data subjects cannot be identified from it.

8. Term, Return and Survival

8.1 This Agreement starts on the Effective Date and continues while the Framework and any SOW remain in force. If the Framework is not signed within 12 months of the Effective Date, this Agreement ends then. Either Party may end it on 30 days' written notice while no SOW is in force.

8.2 Within 30 days after a written request, or when the Purpose ends, the Recipient shall return or securely destroy the Discloser's Confidential Information and certify in writing, within 14 days after the return or destruction, that it has done so. This does not apply to deliverables licensed to the Client under the Framework. The Recipient may keep copies

that the law requires it to retain, and copies held in routine backups until they are overwritten, and those copies stay subject to this Agreement. The Client may instead choose that Personal Data be returned rather than destroyed, unless the law requires retention.

8.3 The obligations of confidentiality survive for 5 years after the later of the end of this Agreement and the last disclosure. However, for trade secrets, the RETACH Methodology and Security Information they continue while the information remains confidential, and for Personal Data and credentials they continue while the Recipient or its Representatives hold them. Clauses 3, 4, 6, 8.2, 9 and 11 survive termination.

9. Remedies and Liability

9.1 Each Party acknowledges that damages alone may not be an adequate remedy for breach of this Agreement, and that the other Party may seek an injunction or other equitable relief without first proving actual loss, at the court's discretion.

9.2 Liability for unauthorised use or disclosure of Confidential Information in breach of this Agreement is not subject to any limit of liability in the Framework or an SOW. Neither Party is liable for loss to the extent it is caused by the other Party, or by the other Party's failure to meet its own obligations under this Agreement or the DPA. Each Party is liable for the acts and omissions of its Representatives under this Agreement.

10. General

10.1 **Entire agreement.** This Agreement, the Framework and each SOW are the whole agreement on their subject matter. If they conflict on confidentiality or Personal Data, this Agreement prevails.

10.2 **Amendment and waiver.** Any change must be in writing and signed by both Parties. A delay or failure to enforce a right is not a waiver of it.

10.3 **Assignment.** Neither Party may assign this Agreement without the other's prior written consent.

10.4 **Severability.** If a provision is held unenforceable, the rest remains in force.

10.5 **Notices.** Notices must be in writing and sent to the address or designated contact each Party gives in the Framework or by written notice.

10.6 **Counterparts.** This Agreement may be signed in counterparts and by electronic signature.

11. Governing Law and Disputes

11.1 This Agreement is governed by the laws of the Republic of Kenya.

11.2 A dispute is first addressed by good-faith negotiation between the Parties' senior representatives for 14 days, then by mediation before a single mediator with costs shared equally. If unresolved, either Party may refer it to the courts of Kenya at Nairobi. Either Party may seek urgent interim relief from the courts at any time.

Execution

Signed by the Parties' authorised signatories on the dates below.

RETACH Digital Ltd	[CLIENT LEGAL NAME]
Name: Paul N. Nduati	Name: _____
Title: Director	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
Witness name: _____	Witness name: _____
Witness signature: _____	Witness signature: _____

Schedule 1 — Personal Data Processing Details

Complete for each SOW that involves Personal Data (clause 6). Locations outside Kenya must be listed here to be consented to under clause 6.7.

Item	Details
Client (controller)	[Client legal name and contact]
RETACH (processor)	RETACH Digital Ltd — [named contact]
Subject matter and purpose	[e.g. security audit / ISO 27001 readiness / policy build under SOW No. ___]
Duration of processing	[per SOW]
Categories of data subjects	[e.g. employees, customers, contractors]
Types of Personal Data	[e.g. names, contact details, user accounts, access logs — state if any sensitive personal data]
Where data is stored and processed	[Kenya / named locations. Any location outside Kenya must be named here and consented to (clause 6.7)]
RETACH tools that hold Client data	[e.g. email, cloud storage, ticketing, hosted analysis tools, with the country where each processes data]
Approved sub-processors	[None / list]
Client contact for personal data breaches	[name, email, phone]