

Annexure B

Non-Disclosure and Confidentiality Agreement

This Non-Disclosure and Confidentiality Agreement ("Agreement") is made effective as of the Effective Date of the Master Services Agreement between PICO (the "PROVIDER" or "Disclosing Party" in respect of its own information, and "Receiving Party" in respect of Client Information) and the CLIENT (the "CLIENT" or "Disclosing Party" in respect of its own information, and "Receiving Party" in respect of PROVIDER Information).

1. OBJECTIVE

The objective of this Agreement is to establish a robust legal framework to protect the Confidential Information (as defined below) shared between the Parties during their business relationship concerning the Public Cloud Services. These obligations ensure that such information is used solely for the purposes agreed upon (i.e., the provision or utilization of Public Cloud Services) and is not disclosed to unauthorized parties, thereby safeguarding the proprietary interests, trade secrets, and intellectual property of the Disclosing Party.

2. CONFIDENTIAL INFORMATION

2.1. Definition

"Confidential Information" means any data or information that is proprietary to any of the Disclosing Party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to:

- 2.1.1. Business and Strategic Information: Any marketing strategies, sales plans, financial information, pricing (including custom pricing, discounts, and billing data), projections, operations, sales estimates, business plans, and performance results relating to the past, present, or future business activities of such party, its Affiliates, subsidiaries, and affiliated companies.
- 2.1.2. Product and Service Information: Plans for products or services, service roadmaps, client or supplier lists, contracts, and service agreements.
- 2.1.3. Technical and System Information (especially for PROVIDER): Any scientific or technical information, invention, design, process, procedure, formula, improvement, technology, methodology, research, and development data. This explicitly includes details about the PROVIDER's cloud infrastructure, network architecture, security protocols, system configurations, specific hardware and software used in delivering Public Cloud Services, internal system vulnerabilities, internal operational procedures, incident response plans, and any proprietary tools or platforms.
- 2.1.4. Software and Data Assets: Any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, algorithms, APIs, access credentials, system logs, performance metrics, resource utilization data, Client-specific configurations, and trade secrets.
- 2.1.5. Client Data (specifically for CLIENT as Disclosing Party): Any Client Data processed, stored, or transmitted through the Public Cloud Services.
- 2.1.6. Other: Any other information that should reasonably be recognized as confidential information of the Disclosing Party, given the nature of the information and the circumstances of disclosure.

2.2. The Receiving Party acknowledges that the Confidential Information is proprietary to the Disclosing Party, has been developed and obtained through significant efforts by the Disclosing Party, and that the Disclosing Party regards all of its Confidential Information as valuable trade secrets.

2.3. Exclusions

Notwithstanding anything in the foregoing to the contrary, Confidential Information does not include information that:

- 2.3.1. Is or becomes part of the public domain without violation of this Agreement by the Receiving Party;
- 2.3.2. Was known to or in the possession of the Receiving Party on a non-confidential basis prior to the disclosure thereof, as evidenced by written records;
- 2.3.3. Was developed independently by the Receiving Party, without the use of or reference to the Confidential Information, as established by written evidence; or

- 2.3.4. Is disclosed to the Receiving Party by a third party under no obligation of confidentiality to the Disclosing Party and without violation of this Agreement by the Receiving Party.
- 2.4. The burden of proving that information may be disclosed because it falls within one of these exclusions shall be on the Receiving Party.
- 2.5. Obligations of the Receiving Party

The Parties recognize that in the course of negotiations, discussions, and/or transactions envisaged between them related to Public Cloud Services, each of them shall be privileged to certain Confidential Information relating to or belonging to the other Party. In consideration of the mutual benefits accruing to the Parties from their association, each Party hereto agrees:

 - 2.5.1. Non-Disclosure: That it shall not, without the prior written permission of the other Party, directly or indirectly disclose or cause to be disclosed any Confidential Information of such other Party to any third party, except as expressly permitted by this Agreement.
 - 2.5.2. Data Protection and Security: That it shall take all reasonable and commercially appropriate technical, administrative, and physical steps and security measures to protect the integrity, confidentiality, and availability of the Confidential Information of the other Party and to ensure against any unauthorized access, use, disclosure, alteration, or destruction thereof. Such measures shall include, but not be limited to, appropriate access controls, data encryption (where applicable and appropriate), secure storage practices, and adherence to industry-standard cybersecurity frameworks relevant to cloud services.
 - 2.5.3. Security Incident Notification: That it shall promptly inform the other Party of any actual or suspected Security Incident or Data Breach involving the Confidential Information of the other Party and shall cooperate fully with the other Party in investigating, containing, and mitigating any such incident, including providing all reasonably requested information.
 - 2.5.4. Third-Party Access: That it shall ensure that all its employees, Affiliates, representatives, sub-contractors, or other persons who are given access to the Confidential Information of the other Party are informed of the confidential nature of the information and are at all times bound by legally valid and direct written non-disclosure obligations on terms no less protective than those contained in this Agreement. The Receiving Party shall be fully responsible for any breach of this Agreement caused by it or by any such employees, representatives, sub-contractors, or other persons to whom it has given access to the Confidential Information of the other Party.
 - 2.5.5. Purpose Limitation: That it shall use the Confidential Information of the other Party only for the specific purpose for which it was provided (i.e., for the provision or utilization of Public Cloud Services as per the Master Services Agreement) and shall not profit from the same in an unauthorized manner to the exclusion of the other Party.
 - 2.5.6. Standard of Care: That it shall treat all Confidential Information of the Disclosing Party with at least the same degree of care as the Receiving Party accords its own Confidential Information of a similar nature, but in no event less than a reasonable standard of care.

3. RETURN AND DESTRUCTION OF CONFIDENTIAL INFORMATION

Upon the termination or expiration of the Master Services Agreement, or at any time demanded by the other Party in writing, each Party shall:

- 3.1. Promptly return to the Disclosing Party (to an authorized representative as intimated by the Disclosing Party) all tangible forms of Confidential Information.
- 3.2. Securely destroy all copies, whether physical or digital, of the Confidential Information in the possession or under the control of the Receiving Party, its employees, or representatives, within seven (7) business days of such request or termination/expiration. For digital data, this shall include verifiable secure erasure methods where feasible, rendering the information unrecoverable.

- 3.3. Provide written confirmation, in the form of a Certificate of Destruction or equivalent, to the Disclosing Party attesting to the complete return and/or destruction of all Confidential Information, as applicable.

4. EXISTENCE

Each Party agrees not to make any press release or otherwise publicize the existence, or any of the terms, of this Agreement, any memorandum of understanding, Agreement or other writing executed between the Parties, or the business relationship itself, without the prior written consent of the other Party.

5. DURATION

- 5.1. The confidentiality obligations shall remain in effect for the duration of the Master Services Agreement.
- 5.2. Notwithstanding anything in Clause 5.1, the Parties' duty to maintain the confidentiality of any Confidential Information disclosed during the term of this Agreement shall remain in effect indefinitely, even after the Master Services Agreement's termination or expiration, for as long as such information retains its confidential nature and has not become part of the public domain through no fault of the Receiving Party.

6. PROPRIETARY RIGHTS

All Confidential Information shall remain the exclusive property of the Disclosing Party. Each Party reserves all rights in its Confidential Information. No rights, including, but not limited to, Intellectual Property rights, in respect of a Party's Confidential Information are granted to the other Party by virtue of this Agreement. Moreover, nothing herein shall in any manner grant a Party any right, title, assignment, license or interest in respect of any Intellectual Property belonging to or devised by the other Party. All the Intellectual Property rights of the respective Parties shall remain the property of such Parties. The Parties shall obtain written approval of the other Party for all advertisements, publications and communications, including or referring to the Intellectual Property rights of the other Party.

7. INDEMNIFICATION

Each Party (the "Breaching Party") shall at all times hereafter indemnify and keep the other Party (the "Non-Breaching Party") fully indemnified against all losses, damages, costs, charges, expenses, interests, and disbursements of any nature whatsoever arising out of third-party claims, demands, actions, or proceedings, which the Non-Breaching Party may pay, incur, suffer or sustain or be liable to pay, incur, suffer or sustain as a result or consequence, direct or indirect, of any breach or failure to perform any of the provisions of this Agreement by the Breaching Party or by its employees, Affiliates, or representatives to whom it has granted access.

8. REMEDIES

Both Parties acknowledge that the Confidential Information to be disclosed hereunder is of a unique and valuable character and that the unauthorized dissemination or misuse of the Confidential Information would cause irreparable harm and significantly destroy or diminish the value of such information. The damage to the Disclosing Party that would result from the unauthorized dissemination or misuse of the Confidential Information would be impossible to calculate. Therefore, both Parties hereby agree that the Disclosing Party shall be entitled to seek injunctive relief preventing the dissemination or misuse of any Confidential Information in violation of the terms hereof. Such injunctive relief shall be in addition to any other remedies available hereunder, whether at law or in equity. The Disclosing Party shall be entitled to recover its costs and fees, including reasonable legal fees, incurred in obtaining any such relief. Further, in the event of litigation relating to this Agreement, the prevailing party shall be entitled to recover its reasonable legal fees and expenses.