The **GOVERNING AGREEMENT** ("Agreement") is entered into on **[Effective Date]** by and between:

PIT Solutions Limited (Formerly Known as PIT Solutions Private Limited), having its registered office at **L7 & L8, Floor (-1), Thejaswini, Technopark, Thiruvananthapuram, Kerala, India, PIN 695 581** (hereinafter referred to as **"PITS"** or the **"Service Provider"**),

and

The **Subscriber** subscribing the PIT Services

PITS and the **Subscriber** are each a **"Party"** and collectively referred to as the **"Parties"** to this Agreement.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties, intending to be legally bound, agree as follows:

1. Definitions

1.1. **"Subscriber"** means the individual or entity subscribing to the PIT services accepting all the Terms of Master Agreement, Terms & Condition and Privacy Policy.

1.2. **"Affiliates"** means, with respect to any entity, any other entity that directly or indirectly controls, is controlled by, or is under common control with such entity. For the purposes of this definition, "Control" means (i) direct or indirect ownership of more than 50% of the voting securities or equity interests, or (ii) the power to direct or cause the direction of the management and policies of such entity, whether through ownership, by contract, or otherwise.

1.3. **"Authorised User"** means any individual for whom the Subscriber has purchased a valid user license pursuant to the terms of the Invoice and this Agreement, and to whom unique user credentials have been issued to access the PITS Services. Authorised Users may include the Subscriber's employees, individual contractors, consultants, Affiliates, or third-party service providers engaged by the Subscriber.

1.4. **"Confidential Information"** means all information disclosed by one party (the **"Disclosing Party"**) to the other party (the **"Receiving Party"**), whether orally, in writing, or by any other means, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of its disclosure.

Without limiting the foregoing:

- PITS's Confidential Information includes, without limitation, the terms of this Agreement, all Invoices (including all non-public pricing and commercial terms), and any related documentation.
- The Confidential Information of each party includes, but is not limited to, business and marketing plans, technology and technical data, product

roadmaps, product designs, software, source code, and business processes disclosed by such party.

Exclusions: Confidential Information does **not** include information that:

- is or becomes publicly available without breach of any obligation owed to the Disclosing Party;
- was lawfully known to the Receiving Party prior to disclosure by the Disclosing Party without breach of any confidentiality obligation;
- is lawfully received from a third party without breach of any confidentiality obligation owed to the Disclosing Party; or
- is independently developed by the Receiving Party without use of, or reference to, the Disclosing Party's Confidential Information.

1.5. **"Documentation"** means any user manuals, guides, technical specifications, release notes, or other instructional materials, whether in written, electronic, or other tangible form, that are provided or made available by PITS to the Subscriber from time to time, describing the features, functionalities, configuration, and operation of the PITS Services.

1.6. **"Deprecation"** means and includes the deprecation, discontinuation, or introduction of any backward-incompatible change to:
(i) the PITS Services;
(ii) any feature or functionality within the PITS Services; or
(iii) any PITS Service APIs.

1.7. **"Non-PITS Services"** means any third-party applications, services, software, networks, systems, websites, or databases (including those accessed through the PITS Marketplace) that are integrated with, or designed to interoperate with, the PITS Services.

1.8. **"Invoice"** means the document issued by PITS evidencing the Subscriber's subscription to the PITS Services, which sets out details including the name of the subscribed PITS Services, the applicable subscription plan, the Subscription Period, the number of user licenses purchased, the applicable fees, and any other specific terms and conditions agreed between the Parties.

1.9. **"Subscriber Data"** means all electronic data, information, or content submitted, uploaded, or otherwise transmitted to, and stored within, the PITS Services by the Subscriber or any Authorised User in connection with their use of the PITS Services

1.10. **"Subscription Period(s)"** means, with respect to each PITS Service, the duration for which the Subscriber has purchased and paid for a fee-based subscription plan, as specified in the applicable Invoice.

1.11. **Usage Limits"** means the restrictions or limits on the use of each PITS Service, including but not limited to the number of users, storage capacity, transactions, or other usage parameters, as specified under the fee-based subscription plan purchased by the Subscriber and set forth in the applicable Invoice.

1.12. **"Taxes"** means all taxes, duties, levies, imposts, charges, or similar governmental assessments of any kind, including without limitation sales, use, value-added, goods and services, excise, business, service, or other transactional taxes, together with any related interest, penalties, or fines, imposed by any local, state, provincial, national, or foreign authority.

1.13. **"Terms of Service"** means the terms and conditions published at **https://www.pitsolutions.com,** together with any additional service-specific terms and conditions published at https://medinotex.ai/, governing the access to and use of the PITS Services, as may be amended or updated by PITS from time to time.

1.14. **"PITS Marketplace"** means the online marketplace for applications that are designed to integrate with and interoperate with the PITS Services.

1.15. **"PITS Services"** means one or more of the hosted software services provided by PITS, as listed in **Exhibit A**, that are purchased by the Subscriber through an Invoice or via an online purchasing portal, and includes any related downloadable or mobile applications.

1.16. **"One-Time Charges"** means fees that may include, but are not limited to, implementation and setup fees, onboarding and training costs, data migration and system integration fees, and any customization or development specifically requested by the Subscriber. Such One-Time Charges shall be invoiced separately from recurring subscription or maintenance fees and shall be payable as per the payment terms mentioned in the invoice or as otherwise agreed in writing between the Parties. Unless expressly stated otherwise in writing, all One-Time Charges are non-refundable.

For clarity, payment of One-Time Charges does not transfer any ownership rights in the underlying software, customizations, or developments to the Subscriber; all intellectual property rights shall remain the exclusive property of PITS, unless otherwise expressly agreed in writing.

1.17. **"Effective Date"** means the date on which the Subscriber either creates an account or pays the Subscription Fees, whichever occurs earlier**.**

2. Use of the PITS Services, Restrictions, and Responsibilities

2.1. Rights Granted

Subject to the terms and conditions of this Agreement and the applicable Invoice, PITS shall make the PITS Services available to the Subscriber for the specified Subscription Period. PITS grants the Subscriber a limited, non-exclusive, non-transferable, and revocable license to access, use, and, where applicable, download the PITS Services solely for the Subscriber's internal business purposes during the Subscription Period.

If the Subscriber exceeds the applicable Usage Limits of the PITS Services or any of its functionalities, the Subscriber shall purchase additional quantities or capacity of the PITS Services by paying the applicable fees for such excess usage, as invoiced by PITS.

2.2. Usage Restrictions.

The Subscriber shall not, and shall ensure that its Authorised Users do not, directly or indirectly:

2.2.1. copy, modify, translate, adapt, or create derivative works based on the PITS Services, or attempt to gain unauthorized access to them;

2.2.2. disassemble, reverse engineer, or decompile the PITS Services, except as expressly permitted under applicable law;

2.2.3. use the PITS Services on behalf of, or for the benefit of, any third party, operate as a service bureau, or provide any business process or outsourcing services using the PITS Services;

2.2.4. use the PITS Services in any manner that interferes with, disrupts, or compromises the integrity, security, or performance of the PITS Services, its components, or any data contained therein;

2.2.5. sell, resell, license, sublicense, rent, lease, transfer, assign, or otherwise make the PITS Services available to any third party, except through properly assigned Authorised User subscriptions;

2.2.6. use the PITS Services to send or store material containing software viruses, worms, Trojan horses, or other malicious code, files, or programs;

2.2.7. use the PITS Services to store, transmit, or process any material that is unlawful, abusive, malicious, harassing, defamatory, obscene, libelous, or otherwise violates applicable laws or third-party rights;

2.2.8. permit direct or indirect access to or use of the PITS Services in a manner that circumvents the agreed Usage Limits;

2.2.9. use the PITS Services in any manner that could damage, disable, overburden, impair, or otherwise harm any PITS server, network, computer system, or resource;

2.2.10. allow Authorised User licenses to be shared or used by more than one individual, except by way of reassigning such license to a new individual replacing a former Authorised User;

2.2.11. remove, alter, or obscure any proprietary rights notices, trademarks, or other ownership markings contained in the PITS Services;

2.2.12. attempt to gain unauthorized access to the PITS Services, including any restricted features or functionality, or to its related systems, networks, or data;

2.2.13. use the PITS Services for any competitive, benchmarking, or comparative analysis purposes, except with PITS's prior written consent.

2.3. Subscriber Responsibilities

The Subscriber shall be responsible for:

2.3.1. providing accurate, current, and complete information about the Subscriber in connection with its access to and use of the PITS Services;

2.3.2. ensuring that all Authorised Users comply with this Agreement, the Documentation, and the applicable Invoice;

2.3.3. the accuracy, quality, legality, and integrity of all Subscriber Data;

2.3.4. ensuring that the Subscriber Data has been lawfully acquired and that the Subscriber's use of such data complies with applicable laws, this Agreement, and all third-party rights;

2.3.5. using commercially reasonable efforts to prevent any unauthorized access to or use of the PITS Services and promptly notifying PITS of any such unauthorized access or use;

2.3.6. using the PITS Services strictly in accordance with this Agreement, the Documentation, and the applicable Invoice;

2.3.7. all activities occurring under the Subscriber's account, whether or not authorized by the Subscriber;

2.3.8. complying with all applicable laws, rules, and regulations in connection with its use of the PITS Services; and

2.3.9. ensuring compliance with all terms and conditions applicable to the use of any Non-PITS Services integrated with the PITS Services.

2.3.10. being solely responsible for any breach of this Agreement caused by its Authorised Users, Affiliates, contractors, or any third-party integrations used in connection with the PITS Services.

2.4. Suspension of Services

PITS may, without liability, temporarily suspend or restrict the Subscriber's or any Authorised User's access to or use of the PITS Services under the following circumstances:

2.4.1. Breach of Agreement – if the Subscriber or any Authorised User violates the terms of this Agreement, including the Usage Restrictions or Subscriber Responsibilities;

2.4.2. Non-Payment – if any fees, including Subscription or One-Time Charges, remain unpaid beyond the applicable due date;

2.4.3. Security Risks – if suspension is reasonably necessary to prevent unauthorized access, maintain the integrity, security, or availability of the PITS Services, or protect PITS's systems, network, or data;

2.4.4. Legal or Regulatory Requirement – if required to comply with applicable laws, regulations, or governmental orders;

2.4.5. Excess Usage – if the Subscriber exceeds the agreed Usage Limits and fails to purchase additional capacity after notification from PITS.

PITS shall make commercially reasonable efforts to provide prior notice to the Subscriber before any such suspension, unless immediate suspension is required for security or legal reasons. Access will be restored promptly once the underlying cause of suspension is resolved

3. Fees and Payments

3.1. Fees

The Subscriber shall pay to PITS, without any deductions or set-offs, the fees specified in the applicable Invoice. Except as expressly stated in this Agreement:

- all payment obligations are non-cancellable;
- all amounts paid are non-refundable, whether or not the PITS Services are actively used; and

- additional charges shall apply for any additional purchases or usage in excess of the subscribed quantities.

All pricing terms shall be treated as confidential information, and the Subscriber shall not disclose such terms to any third party without PITS's prior written consent.

3.2. Invoicing and Payment

The Subscription Period shall commence only upon PITS's receipt of full payment or a purchase order acceptable to PITS.

The Subscriber shall

- provide complete and accurate payment information to PITS; and
- promptly update PITS regarding any changes to such information.

3.3. One-Time Charges

Upon mutual agreement of the Parties, PITS shall issue an invoice for any applicable One-Time Charges. The Subscriber shall adhere to terms mentioned in the invoicing and payment clause mentioned in clause 3.2

3.4. Overdue Payments

Undisputed overdue amounts shall accrue interest at the rate of one percent (1%) per month or the maximum rate permitted under applicable law, whichever is lower.

Failure to pay any undisputed fees within the timeline specified in the applicable Invoice shall constitute a material breach of this Agreement, entitling PITS to:

- downgrade the Subscriber's account to a free or limited-access plan of the applicable PITS Service until all outstanding undisputed amounts (including accrued interest) are paid in full; and/or
- terminate this Agreement in accordance with Clause 12.2.

3.5. Payment Disputes

The Subscriber must raise any disputes regarding an invoice within five (5) business days of receipt of such invoice. The Subscriber shall not be considered in default of its payment obligations if:

- the disputed amount is being challenged in good faith in accordance with this Clause, and the Subscriber is cooperating diligently to resolve the dispute; and
- all undisputed amounts are paid in accordance with this Agreement.

3.6. Taxes

The Subscriber shall be responsible for all applicable Taxes, in addition to the fees for the PITS Services, as specified in the Invoice. If the Subscriber is required to withhold any Taxes, it shall remit such withholding tax/ applicable Tax directly to the appropriate governmental authority and shall provide PITS with a valid tax certificate evidencing such payment.

3.7. Pricing

PITS reserves the right to determine and modify its pricing for the PITS Services at its sole discretion. However, where an Invoice is in effect, the

pricing agreed therein shall remain valid for the duration of the Subscription Period specified in such Invoice.

4. Availability and Technical Support

4.1. Service Availability

PITS shall make the PITS Services available to the Subscriber in accordance with the terms of this Agreement, the applicable Invoice, and the Documentation. PITS shall use commercially reasonable efforts to make the PITS Services available 24 hours a day, 7 days a week, and shall honour the Monthly Uptime Commitment set forth in **Exhibit B**, except in the following circumstances:

- Scheduled Downtime, notified in advance by PITS; and
- Force Majeure Events as defined under this Agreement.

4.2. Support

The support commitments provided by PITS are described in **Exhibit C**. PITS shall respond to and resolve any Service Defects reported by the Subscriber in accordance with the response and resolution timeframes specified in **Exhibit C.**

5. Privacy and Security

5.1. Privacy

To the extent that Personal Information is processed by PITS in connection with the Subscriber's use of the PITS Services, PITS shall comply with all applicable privacy, data protection, and confidentiality laws and regulations. PITS's processing of Personal Information shall, at all times, be in accordance with **Exhibit E** of this Agreement, which specifies how PITS will:

- process Personal Information;
- engage third-party service providers to process Personal Information on its behalf;
- assist the Subscriber in responding to data subject requests;
- manage and report Security Incidents;
- accommodate audit requests from the Subscriber (where applicable);
- ensure its personnel maintain the confidentiality and security of Personal Information; and
- manage the return or deletion of Personal Information upon termination or expiry of this Agreement.

5.2. Security

PITS shall implement and maintain industry-standard administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Subscriber Data, as described in **Exhibit D** of this Agreement. PITS shall periodically review and update its security practices to address evolving security threats, industry standards, and emerging security technologies. PITS warrants that no changes to its security practices will materially degrade the security of the PITS Services.

5.3. Protection of Electronic Personal Health Data

The security and privacy of any Electronic Personal Health Data belonging to PITS, its employees, or its customers/ Subscriber shall be protected in accordance with applicable healthcare privacy and data protection laws, including, where applicable, the Health Insurance Portability and Accountability Act (HIPAA), PITS shall apply the same safeguards described in Clause 5.1 and 5.2 to such data and shall ensure that any third-party service providers engaged in processing such data comply with equivalent standards.

6. Non-PITS Services

6.1. Access and Use

From time to time, PITS and/or third parties may make available certain Non-PITS Services. If the Subscriber chooses to enable, access, or use such Non-PITS Services, the Subscriber's access to and use of such services shall be governed exclusively by the applicable terms and conditions of those Non-PITS Services. The Subscriber shall be solely responsible for reviewing, accepting, and complying with such terms prior to accessing or using any Non-PITS Services.

6.2. Disclaimer of Liability

PITS does not endorse, support, or make any representations or warranties regarding any aspect of the Non-PITS Services. PITS shall have no liability or responsibility for any damage, loss, or other liability (including any loss or corruption of Subscriber Data) arising from or in connection with the Subscriber's access to or use of such Non-PITS Services.

6.3. Availability

PITS does not guarantee the continued availability of any Non-PITS Services or of any features or functionalities within the PITS Services that are designed to interoperate with such Non-PITS Services.

7. Proprietary Rights and Licenses

7.1. Reservation of Intellectual Property Rights

As between the Parties, PITS retains all rights, title, and interest in and to the PITS Services, Documentation, and any related deliverables, including all associated intellectual property rights. Except as expressly granted under this Agreement, no rights or licenses are conferred to the Subscriber in respect of the PITS Services or any of PITS's intellectual property, including but not limited to its source code, system architecture, features, branding, documentation, proprietary algorithms, or trade secrets.

7.2. Ownership of Customizations and Deliverables

Any customizations, enhancements, modifications, or deliverables developed or provided by PITS under this Agreement shall remain the exclusive property of PITS, including all associated intellectual property

rights, unless expressly agreed otherwise in a separate written agreement executed by the Parties.

The Subscriber is granted only a limited, non-exclusive, non-transferable license to use such customizations or deliverables solely for its internal business purposes during the Subscription Period, subject to the terms of this Agreement.

7.3. Subscriber Restrictions

The Subscriber agrees that it shall not, and shall ensure its Authorised Users do not:

7.3.1. reproduce, modify, distribute, or create derivative works of the PITS Services or Documentation without PITS's prior written consent;

7.3.2. use the PITS Services to develop or offer any competing product or service;

7.3.3. attempt to reverse engineer, decompile, disassemble, or otherwise attempt to extract any part of the proprietary system, source code, or algorithms of the PITS Services; and

7.3.4. claim ownership of or any intellectual property rights in any customizations, enhancements, or deliverables provided by PITS.

7.4. License to Use Suggestions and Feedback

The Subscriber grants PITS a fully paid-up, royalty-free, worldwide, transferable, sub-licensable, irrevocable, and perpetual license to use, copy, modify, and incorporate into the PITS Services any ideas, suggestions, enhancement requests, recommendations, corrections, or other feedback provided by the Subscriber in connection with its use of the PITS Services.

7.5. Intellectual Property Indemnity

PITS shall have no liability or indemnification obligation for claims to the extent arising from:

- modifications to the PITS Services made by or on behalf of the Subscriber without PITS's written authorization;
- use of the PITS Services in combination with Non-PITS Services, third-party products, or services not provided or approved by PITS;
- use of the PITS Services outside the scope of this Agreement or in violation of applicable law; or
- the Subscriber's data, content, or other materials provided to PITS.

8. Confidentiality

8.1. Confidentiality Obligations

- Except as expressly permitted in writing by the Disclosing Party, the Receiving Party shall:
- use the same degree of care it uses to protect its own confidential information of a similar nature (but in no event less than a reasonable standard of care) to protect the Confidential Information of the Disclosing Party;

- not use any Confidential Information of the Disclosing Party for any purpose other than as necessary to perform its obligations or exercise its rights under this Agreement; and
- restrict disclosure of Confidential Information of the Disclosing Party to only those of its employees, contractors, or agents who have a legitimate need to know such information for purposes consistent with this Agreement, provided that such persons are bound by confidentiality obligations no less protective than those set forth herein.
- Any Confidential Information exchanged between the Parties prior to the execution of this Agreement shall continue to be governed by any existing non-disclosure agreement between the Parties, and not by this Agreement.
- Upon the earlier of (a) written request by the Disclosing Party, or (b) expiration or termination of this Agreement for any reason, the Receiving Party shall promptly return or securely destroy all copies of Confidential Information (regardless of form), except where retention is required by applicable law or permitted for archival or compliance purposes, in which case the information shall remain subject to the confidentiality obligations hereunder.

8.2. Compelled Disclosure

The Receiving Party may disclose Confidential Information of the Disclosing Party only:

- to the extent required by a valid order or subpoena of a court or governmental authority;
- as reasonably necessary to comply with applicable law or regulation; or
- as necessary to establish or defend its legal rights in a proceeding,

provided that (a) the Receiving Party gives prior written notice to the Disclosing Party (to the extent legally permitted) to allow it to seek a protective order or other appropriate remedy, and (b) the disclosure is limited strictly to the minimum information required and remains subject to confidentiality protections to the extent reasonably practicable.

9. Representations, Warranties, and Disclaimers

9.1. Mutual Representation

Each Party represents and warrants to the other that:

- it is duly organized, validly existing, and in good standing under the laws of its jurisdiction of incorporation;
- it has the full corporate power and authority to enter into this Agreement; and
- its execution and performance of this Agreement have been duly authorized and will not violate any applicable law or agreement to which it is bound.

9.2. Warranty by PITS

PITS warrants that, during the applicable Subscription Period:

- the PITS Services will perform substantially in accordance with the Documentation, provided the Subscriber uses the Services in accordance with such Documentation;
- PITS will maintain administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Subscriber Data, as described in **Exhibit D**; and
- subject to the "Non-PITS Services" clause and except in cases of Deprecation, PITS will not materially decrease the overall functionality of the PITS Services.
- In the event of any breach of the warranties set out in this clause, the Subscriber's sole and exclusive remedies shall be as described in Clause 12.2 and 12.3 of this Agreement.

9.3. Deprecation

PITS shall announce any Deprecation at least three (3) months prior to its effective date (the "Deprecation Period") and shall, where commercially reasonable, recommend alternative solutions.

During the Deprecation Period, the Subscriber may terminate this Agreement with immediate effect and shall be entitled to a pro-rata refund of subscription fees for the unused portion of the Subscription Period. Upon request, PITS shall provide the Subscriber with a complete export of data to facilitate migration.

9.4. Warranty Disclaimer

Except as expressly provided in this Agreement, the PITS Services are provided "as is" and "as available" without any warranties of any kind. To the maximum extent permitted by applicable law, PITS disclaims all other warranties, express, implied, statutory, or otherwise, including but not limited to implied warranties of merchantability, title, fitness for a particular purpose, and non-infringement.

PITS does not warrant that the Services will be uninterrupted, timely, secure, error-free, or free from viruses or other harmful code. No advice or information obtained from PITS or third parties shall create any warranty not expressly stated herein.

The foregoing exclusions and limitations shall apply even if any remedy fails of its essential purpose.

9.5. Disclaimer – Third-Party Professional Services

If the Subscriber avails itself of professional services (including implementation, integration, optimization, or customization) from third-party service providers, including consulting partners listed on PITS's website ("Third Party Service Providers"), PITS shall not be liable for any acts, omissions, or deficiencies in services rendered by such Third Party Service Providers.

9.6. Disclaimer – AI Functionality and Clinical Responsibility

9.6.1. The PITS Services may include AI-assisted features designed solely to assist in clinical workflows, documentation, and analysis. Such features are advisory tools and are not intended to replace, override, or substitute professional medical judgment, diagnosis, or decision-making.

9.6.2. The Subscriber expressly acknowledges and agrees that:

9.6.2.1. all clinical and medical decisions remain the sole responsibility of qualified and licensed healthcare professionals using the PITS Services;

9.6.2.2. the Subscriber and its authorized users shall independently verify any AI-generated suggestions, insights, or analysis before relying upon them in a clinical or medical context;

9.6.2.3. PITS shall have no liability whatsoever for any medical, diagnostic, or treatment-related outcomes, adverse events, or other consequences resulting from the Subscriber's or its users' reliance on AI-assisted features; and

9.6.2.4. the Subscriber assumes full responsibility for ensuring that its users are adequately trained and competent in the use of AI-assisted tools.

9.6.3. The PITS Services maintain logs, version histories, and data traceability to ensure transparency of AI-generated content; however, such records are provided solely for audit and traceability purposes and do not create any additional warranty or obligation on PITS beyond those expressly stated in this Agreement.

9.6.4. **Subscriber Indemnity.** The Subscriber shall indemnify, defend, and hold harmless PITS, its affiliates, and their respective officers, directors, employees, and agents from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to:

(a) the Subscriber's or its authorized users' reliance on AI-assisted features in making clinical or medical decisions; and

(b) any medical, diagnostic, or treatment-related outcomes resulting from such reliance.

10. Indemnification

10.1. Indemnification by PITS

10.1.1. **Intellectual Property Indemnity**

PITS shall defend the Subscriber against any third-party claim, demand, suit, or proceeding alleging that the PITS Services, when used by the Subscriber in accordance with this Agreement, infringe or misappropriate any third party's intellectual property rights ("Claim"). PITS shall indemnify and hold harmless the Subscriber from:

(i) any damages or costs (including reasonable attorneys' fees) finally awarded against the Subscriber by a court of competent jurisdiction; or

(ii) amounts agreed to in a settlement approved by PITS, provided that the Subscriber:

(a) promptly provides written notice of the Claim to PITS;

(b) grants PITS sole and exclusive control over the defense and settlement of the Claim (provided that PITS will not settle any Claim unless the settlement unconditionally releases the Subscriber of all liability); and

(c) provides all reasonable cooperation and assistance, at PITS's expense.

10.1.2. Remedies for Infringement Claims

If a Claim is made, or in PITS's opinion is likely to be made, PITS may, at its sole discretion and expense:

(i) obtain a license permitting the Subscriber to continue using the affected PITS Services;

(ii) replace or modify the PITS Services to make them non-infringing without materially diminishing their functionality; or

(iii) if neither (i) nor (ii) is commercially reasonable, terminate the affected PITS Services upon thirty (30) days' written notice and refund any prepaid fees for the unused portion of the Subscription Period.

Clauses 10.1.1 and 10.1.2 set forth PITS's entire liability and the Subscriber's sole and exclusive remedy for third-party intellectual property infringement claims

10.1.3. Exclusions

PITS shall have no liability or indemnification obligation for any Claim to the extent arising from:

(i) modifications to the PITS Services made by the Subscriber or any party authorized by the Subscriber;

(ii) use or combination of the PITS Services with third-party products, software, or services not provided or authorized by PITS;

(iii) use of the PITS Services in violation of this Agreement or applicable law;

(iv) use of the PITS Services inconsistent with the applicable Documentation; or

(v) any Non-PITS Services.

10.2. Indemnification by Subscriber

10.2.1. **Subscriber's Indemnity**

The Subscriber shall defend, indemnify, and hold harmless PITS, its affiliates, and their respective officers, directors, employees, and agents against any third-party claim, demand, action, or proceeding arising from or related to:

(i) the Subscriber's or its authorized users' use of the PITS Services in violation of this Agreement or applicable law; or

(ii) the Subscriber's Data or content, including any claim that such data infringes or misappropriates a third party's intellectual property rights or violates applicable law.

The Subscriber shall indemnify PITS for all damages, costs, and reasonable attorneys' fees finally awarded or agreed in a settlement approved by the Subscriber, provided that PITS:

(a) promptly notifies the Subscriber in writing of the claim;

(b) grants the Subscriber sole control over the defense and settlement of the claim (provided that the Subscriber shall not settle any claim unless the settlement unconditionally releases PITS from all liability); and
(c) provides all reasonable cooperation and assistance, at the Subscriber's expense.

10.2.2. **Exclusion**

The Subscriber shall not be obligated to indemnify PITS for any claim arising solely due to PITS's breach of this Agreement, the Documentation, or the applicable Invoice.

11. Limitation of Liability

11.1. Exclusion of Certain Damages

To the maximum extent permitted by applicable law, under no circumstances and under no legal theory—whether in contract, tort (including negligence), strict liability, product liability, or otherwise—shall either Party or its affiliates be liable to the other Party, its affiliates, or any third party for:
(i) any loss of profits, revenue, sales, business, or goodwill;
(ii) any loss, corruption, or deletion of data (except where caused solely by PITS's gross negligence or wilful misconduct);
(iii) any business interruption; or
(iv) any indirect, incidental, special, exemplary, consequential, or punitive damages,
even if such Party has been advised of the possibility of such damages, and even if any limited remedy fails of its essential purpose.

11.2. Cap on Financial Exposure

Except for (a) the Subscriber's payment obligations under this Agreement, (b) either Party's indemnification obligations under Clause 10, and (c) either Party's breach of confidentiality obligations under Clause 8, each Party's total cumulative liability to the other Party and its affiliates, for any claim or series of related claims arising out of or related to this Agreement, shall not exceed the total fees actually paid by the Subscriber to PITS in the twelve (12) months immediately preceding the first event giving rise to such claim ("Liability Cap").

11.3. Fees Unaffected

The limitations set forth in this clause shall not affect the Subscriber's obligation to pay all fees due in accordance with this Agreement.

12. Term and Termination

12.1. Term

This Agreement shall commence on the Effective Date and continue for the duration of the Subscription Period specified in the applicable Invoice, unless earlier terminated in accordance with this clause. Except as otherwise stated in this Agreement or the applicable Invoice, subscriptions shall automatically renew for successive terms equal to the expiring

Subscription Period, unless either Party provides written notice of non-renewal at least thirty (30) days before the end of the then-current term.

12.2. Termination for Cause

Either Party may terminate this Agreement for cause:

(i) **Material Breach** – Upon fifteen (15) days' prior written notice to the other Party of a material breach, if such breach remains uncured at the end of such notice period.

(ii) **Insolvency** – Immediately, if the other Party becomes the subject of bankruptcy, insolvency, receivership, liquidation, or any similar proceeding, or makes an assignment for the benefit of creditors.

(iii) **Non-Payment** – PITS may immediately suspend or terminate the Subscriber's access to the PITS Services if any undisputed fees remain unpaid for more than thirty (30) days after the due date, following written notice.

12.3. Termination for Convenience (Subscriber)

The Subscriber may terminate this Agreement for any reason or no reason by providing thirty (30) days' prior written notice to PITS.

(a) **Refund** – In such event, PITS shall refund prepaid fees for the unused portion of the Subscription Period, after deducting early termination charges, if applicable.

(b) **Early Termination Charges** – Unless otherwise agreed in writing, the Subscriber shall pay PITS an early termination charge equal to one (1) month of subscription fees or 10% of the remaining Subscription Period fees (whichever is higher) to cover administrative and service costs.

12.4. Export and Deletion of Subscriber Data

Upon termination or expiration:

(i) PITS shall make Subscriber Data available for electronic retrieval for thirty (30) days in a commonly used, machine-readable format.

(ii) After such period, PITS may permanently delete all Subscriber Data from its active systems, and backup data shall be deleted within three (3) months thereafter.

(iii) Accounts that remain unpaid and inactive for 120 consecutive days may be terminated by PITS after giving prior written notice.

12.5. Post-Termination Assistance

If requested in writing by the Subscriber before or within the 30-day retrieval period, PITS may provide reasonable data migration or transition assistance, subject to availability and at PITS's then-current professional service rates.

12.6. Surviving Provisions

The following provisions shall survive termination or expiration: Confidentiality, Fees and Payments, Warranty Disclaimers, Limitation of Liability, Indemnification, Termination, Surviving Provisions, and General Provisions.

12.7. Effect of Termination

Upon termination or expiration of this Agreement:

- all rights and licenses granted under this Agreement shall immediately cease;
- the Subscriber shall immediately stop using the PITS Services, unless otherwise agreed in writing; and
- each Party shall return or destroy the other Party's Confidential Information in accordance with Clause 8.

13. General

13.1. Applicability of Terms of Service

The Subscriber acknowledges that, in addition to the terms of this Agreement, the PITS Terms of Service shall apply to the Subscriber's access and use of the PITS Services. In the event of any conflict between this Agreement and the Terms of Service, the terms of this Agreement shall prevail.

13.2. Entire Agreement

This Agreement, together with the attached Exhibits and the Terms of Service, constitutes the entire agreement between the Parties regarding the subject matter hereof and supersedes all prior and contemporaneous agreements, proposals, negotiations, communications, and understandings, whether written or oral, relating to such subject matter.

13.3. Amendment

No modification, amendment, or waiver of any provision of this Agreement shall be effective unless made in writing and signed by the duly authorized representatives of both Parties.

13.4. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of India, excluding its conflict-of-laws principles. Any dispute arising under or in connection with this Agreement shall be subject to the exclusive jurisdiction of the competent courts in Thiruvananthapuram Kerala, India.

13.5. Notices

All notices or other communications under this Agreement shall be in writing and delivered:

(i) by hand;

(ii) by overnight courier;

(iii) by registered or certified mail with return receipt requested;

(iv) by facsimile transmission (with a confirmatory copy sent by courier or mail); or

(v) by electronic mail.

Notices shall be deemed received:

(a) if delivered by hand, upon delivery;

(b) if sent by overnight courier, on the next business day;

(c) if sent by registered or certified mail, on the date of receipt as evidenced by postal records;
(d) if sent by facsimile, upon confirmation of successful transmission (subject to the confirmatory copy requirement); and
(e) if sent by email, upon transmission, provided no bounce-back or error message is received.
Notices shall be sent to:

If to PITS: support@medinotex.ai

If to Subscriber: The Mail ID in which the account is created

Each Party may change its notice address by providing written notice to the other Party.

13.6. Relationship of the Parties

The Parties are independent contractors. Nothing in this Agreement shall be construed to create a partnership, joint venture, franchise, agency, fiduciary, or employment relationship. Neither Party is authorized to bind the other or incur obligations on the other Party's behalf without prior written consent.

13.7. Assignment

Neither Party may assign, delegate, or transfer this Agreement, in whole or in part, without the prior written consent of the other Party, which consent shall not be unreasonably withheld, conditioned, or delayed.
Notwithstanding the foregoing, either Party may assign this Agreement without the other Party's consent:
(i) to an Affiliate; or
(ii) in connection with a merger, consolidation, or sale of substantially all its assets or equity.
Any assignment in violation of this clause shall be void.

13.8. No Third-Party Beneficiaries

This Agreement is intended solely for the benefit of the Parties and their respective successors and permitted assigns. No third party shall have any rights or remedies under this Agreement.

13.9. Force Majeure

13.9.1. **Force Majeure Event**

Neither Party shall be liable for any failure or delay in performing its obligations under this Agreement if such failure or delay results from causes beyond its reasonable control, including but not limited to acts of God, natural disasters, pandemics, acts of war or terrorism, strikes, labour disputes, government actions, or widespread internet or telecommunications outages not caused by the affected Party ("Force Majeure Event").

13.9.2. **Notice and Termination**

The affected Party shall promptly notify the other Party of the occurrence of a Force Majeure Event and shall use reasonable efforts to mitigate its effects. If the Force Majeure Event continues for more than thirty (30)

consecutive days, either Party may terminate this Agreement or any affected Invoice upon written notice.

13.10. Severability

If any provision of this Agreement is held invalid or unenforceable by a court of competent jurisdiction, such provision shall be interpreted to best achieve its original intent to the maximum extent permitted by law, and the remaining provisions shall remain in full force and effect.

13.11. Waiver

No failure or delay by either Party in exercising any right under this Agreement shall operate as a waiver of that right. Any waiver must be in writing and signed by the Party granting it, and shall not constitute a continuing waiver unless expressly stated.

13.12. Interpretation

No provision of this Agreement shall be construed against a Party solely because it was the drafter of the Agreement. Headings are for convenience only and shall not affect the interpretation of any provision.

Exhibit A

PITS SERVICES

1. Overview

MediNoteX AI, developed by PITS, is an AI-powered medical screening and transcription platform. It automates the extraction, structuring, and summarization of patient data from a variety of medical documents, including prescriptions, clinical notes, and laboratory reports. The system assists healthcare professionals by providing fast, accurate, and structured insights from unstructured text using Optical Character Recognition (OCR) and large language models (LLMs).

2. Scope of Services

- Under this engagement, PITS will provide the following services for MediNoteX AI:

a. Product Implementation and Deployment

- Installation, configuration, and environment setup (on Azure or client infrastructure).
- Integration of backend services.
- Secure deployment using Docker and Azure Web App.

b. Maintenance and Support

- Ongoing monitoring and error resolution.
- Regular product updates and feature enhancements.
- Security patches and performance optimization.

c. Training & Documentation

- Product training for end users and administrators.
- Technical documentation, including API usage guides and feature manuals.

d. Other Terms and Conditions

- OpenAI subscription/licensing to be procured separately.
- This is a custom plan, distinct from the standard SaaS offering, allowing unlimited transcriptions per month.
- Client retains ownership of all patient data.
- PITS may release updates and new features periodically.
- Client will be notified in advance of significant changes.

Exhibit B

SERVICE LEVEL TERMS AND CONDITIONS

"Downtime" shall mean inability to access PITS Services due to a Qualifying Fault. Downtime is measured based on availability of the individual PITS Services as measured by PITS's application monitoring tool.

"Qualifying Fault" shall mean and include server side errors and reachability errors attributable to PITS Services.

"Downtime Period" shall mean ten or more consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

"Monthly Uptime" shall mean total number of minutes in a calendar month minus the number of minutes of Downtime suffered from all Downtime Periods in a calendar month.

"Monthly Uptime Percentage" shall mean the percentage calculated by dividing Monthly Uptime by the total number of minutes in a calendar month.

"Scheduled Downtime" shall mean unavailability of PITS Services about which Subscriber is informed at least forty eight (48) hours in advance. A Schedule Downtime will not constitute a Qualifying Fault.

Planning of Scheduled Downtime: PITS will ensure that Scheduled Downtime is planned on weekends between 9:00 pm to 6:00 am (Pacific Time in the United States).

Monthly Uptime Commitment: PITS Services will have a Monthly Uptime Percentage of 99.9%.

SLA Exclusions. The SLA does not apply to any performance and availability issues: (i) caused by factors outside of PITS's reasonable control; (ii) that resulted from any actions or inactions of Subscriber; or (iii) that resulted from Subscriber's equipment and/or third party equipment that are not within PITS's reasonable control. It is hereby clarified that performance and availability issues caused by factors within PITS's control and attributable to PITS or its vendors are not excluded.

REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK

Exhibit C

SUPPORT TERMS AND CONDITIONS

(About the product)

MediNoteX AI provides automated medical documentation, AI-assisted screening, and integration support for healthcare workflows. The following terms define the scope, response, and service levels for support and maintenance.

Our Data Privacy Officer oversees the triage process, assigns priority levels, and ensures that issues are resolved in a timely manner. All incidents are recorded in our Incident Response Sheet, which has a mandatory resolution timeline of 60 days.

For Data Privacy, The client can contact nidhin.a@pitsolutions.com

Irrespective of the support plans chosen, support for issues reported will be as follows:

Severity Level 1 (Critical): The PITS Service does not function without a fix being applied and the problem has significant effect on the revenues or business operations of Subscriber. A case where there is a total loss of service or a major malfunction impacting patient care, clinical workflows, or compliance. There is no workaround available for the business to run.

Severity Level 2 (High): The PITS Service can function. However, the PITS Service functions providing incorrect results or its performance is inconsistent with the performance described in the Documentation. This is a case where partial loss of functionality that affects key clinical or administrative operations. A workaround may exist but is inefficient.

Severity Level 3 (Medium): The functionality of the PITS Service is not affected by the problem or can be achieved by using other features of the PITS Service. This is a case where there would be design/UI issues, minor operation issues, user guidance questions, or functionality requests that do not impact immediate operations.

Response, Problem Determination and Resolution/Restoration/Work-around Timeframe

Severity Level	Response	Problem Determination	Resolution/Restoration/ Work-around
1	1-2 hours	Issue isolated and root cause identified within 1–2 business days	1-2 business days
2	16-24 hours	Issue analyzed and cause determined within 2–3 business days	2-3 business days
3	5-7 Working days	Root cause identified within 3–5 business days	3-5 business days

- All response and resolution timelines mentioned in this Agreement shall be interpreted in accordance with the standard working hours of the Service Provider's support team, which are 9:00 AM to 6:00 PM IST, Monday through Friday, excluding public holidays observed in India.
- Any issue reported outside these working hours will be considered as logged at 9:00 AM IST on the next working day.
- Resolution timeframes will be counted only during the official working hours, and will not include weekends or public holidays unless otherwise specified for Severity 1 issues
- Even for Severity issues -1, Working hours will be considered as 9:AM to 6 PM IST, if any issues raised after 6 PM, it will be considered as logged at 9 AM next day.
- The incident shall be informed to the entire account leadership, and additionally the client shall receive hourly status updates until full resolution if the same is not resolved as per the specified time mentioned above

- For any communication the Dedicated Account Manager will be as

  Name: Amina Z

  Phone Number: +91 9495628026

  Email Mail ID: amina.z@pitsolutions.com

The change in account Manager will be communicated by PITS through Official mail.

In the event of any data breach or security incident, the PITS shall:

Level	Name of the person	Designation	Email Address
Level 1	Shajna Musthafa	Project Manager	shajna.ma@pitsolutions.com
Level 2	Amina Z	BU Head	amina.z@pitsolutions.com
Level 3	Jazna Rafeek	COO	jazna@pitsolutions.com

- Notify the subscriber promptly within the timeframe defined in the SLA
- Provide details of the breach, affected components, mitigation steps, and remediation actions
- Cooperate with the Subscriber in any forensic investigations or external reporting

In the event that the resolution for any issue is not completed within the specified timeframes. The issue shall be automatically escalated to the next level of management as mentioned in the escalation matrix mentioned below:

REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK

Exhibit D

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

PITS has established, and will maintain at a minimum, an information security management system that includes the following:

1. Infrastructure Security

- PITS has a dedicated Network Operations Center (NOC), which operates 24x7 monitoring the infrastructure health.
- Establishment and implementation of firewall rules in accordance to identified security requirements and business justifications.
- Review of firewall rules on a quarterly basis to ensure that legacy rules are removed and active rules are configured correctly.
- Clear separation of production, development and integration environments to ensure that production data is not replicated or used in non-production environments for testing purposes.
- Management of access to production environments by a central directory and authentication for such access using a combination of strong passwords, two-factor authentication, and passphrase- protected SSH keys. Access to the production environment is facilitated through a separate network with strict rules.
- Deployment of DDOS mitigation capabilities from well established service providers to prevent volumetric attacks and to keep the applications available and performing.

2. Risk Management

- The Service Provider shall conduct an enterprise-wide risk assessment at least annually to identify, evaluate, and prioritize risks to the confidentiality, integrity, and availability of systems and data.
- Internal audit procedures shall be established and executed at defined intervals to assess the effectiveness of information systems and operational processes. Audit findings shall be documented and reported to appropriate stakeholders.

- The Service Provider shall assess the design and operating effectiveness of its security controls against an established control framework. Identified deficiencies shall be tracked to resolution through a formal corrective action process.

3. Secure Software Development process

- Well defined security process that is implemented and monitored throughout the process taking into consideration confidentiality, availability and integrity requirements.
- Implementation of secure software development policies, procedures, and standards that are aligned to industry standard practices.
- Training on secure coding principles and industry standards to personnel involved in the development and coding of products.
- Appropriate checking and elimination procedures to ensure that the service is not affected by malware/viruses during development, maintenance and operation.
- Maintenance of clear distinction between the development, QA and production environments.
- Appropriate security controls to ensure the confidentiality, integrity and availability of the CI/CD pipeline in the software development environment used to develop, deploy, and support the products.

4. Data Security and Management

- Information classification scheme with data handling guidelines related to access control, physical and electronic storage, and electronic transfer.
- Logical separation of each subscriber's service data from other subscriber' data by distributing and maintaining separate logical cloud space for each subscriber.
- Deletion of data from active database upon termination of PITS Services by the subscriber (clean-up occurs once in every 6 months), deletion of backup data within 3 months of deletion from active database and termination of accounts that remain unpaid and inactive for a continuous period of 120 days by giving prior notice to the subscriber.
- Data Encryption: Encryption of sensitive Personal Information at rest using 256 bit Advanced Encryption Standard (AES) .All user credentials and stored

patient data are encrypted before being saved to the database.

- Minimal Data Storage: The system is designed to store only essential patient data to minimize exposure risk.
- Session Handling: Sessions are automatically terminated after prolonged inactivity or multiple failed login attempts to prevent credential misuse. The session is securely stored.
- Access Controls: All external access is strictly authenticated to ensure only authorized personnel can interact with sensitive data. 5. Incident Management Workflow
- An incident response plan and program containing procedures that are to be followed in the event of an information security incident. Dedicated email (support@medinotex.ai) to which external parties can report security incidents and creating awareness among employees to report any potential security incident or weakness on time without any delay.
- Tracking of security incidents, fixing of such incidents through appropriate actions, maintenance of such records in the incident registry and implementation of controls to prevent recurrence of similar incidents.
- Incident management procedures that lays down the steps for notifying the client, and other stakeholders in a timely manner in accordance with breach notification obligations.
- Implementation of appropriate forensic proceed and presentation of evidence in the event of an information security incident likely to result in a legal action**.**

6. Third-Party Vendor Management

Vendor management policy through which PITS evaluates and qualifies third party vendors as a part of which new vendors are onboarded only after understanding their processes and performing risk assessments.

- Execution of agreements with vendors that require vendors to adhere to confidentiality, availability, and integrity commitments in order to maintain PITS's security stance.
- Annual reviews to monitor the operation of vendor's processes and security measures.
- Compliance Commitment

The PITS affirms commitment to comply with applicable data protection and privacy

laws which relates to applicable products, including as on date of signing of this agreement

HIPAA (USA)

ISO 27001: 2022

ISO 9001: 2015

Where applicable, the PITS shall adhere to data residency requirements based on the Client's geographical location, ensuring storage and processing of data in compliant regions.

4. EMR/EHR Integration and FHIR Compatibility

PITS Service which relates to Health care product is built with future capabilities to support integration with leading Electronic Medical Record (EMR) and Electronic Health Record (EHR) systems such as:

- Epic
- Cerner
- Government Health Record Frameworks

The platform is designed to be FHIR-compliant to ensure seamless interoperability with healthcare data exchange standards.

5. Encryption and Security Measures

PITS Service employs stringent security practices to protect sensitive patient and user data, including:

- Encryption at Rest using 256-bit AES (Advanced Encryption Standard)
- Encryption in Transit using TLS/SSL protocols
- Authentication & Access Controls via Multi-Factor Authentication (MFA) and Single Sign-On (SSO)
- Regular Backups with retention and recovery plans
- Role-Based Access Controls (RBAC) to restrict data access based on user roles
- All stored user credentials and patient data are securely encrypted before being written to the database

6. Security Governance

- The Service Provider shall maintain a documented governance framework that supports the implementation, oversight, and continuous improvement of information security policies, standards, and controls across the organization.

- Roles and responsibilities related to information security shall be formally defined, approved by management, and communicated to relevant personnel to ensure accountability and alignment with governance objectives.
- An information security program shall be maintained in accordance with internationally recognized standards such as ISO/IEC 27001, encompassing technical, organizational, and physical safeguards to protect Personal Information and Client Data from unauthorized access, loss, or misuse.
- Core policies, including but not limited to information security, data privacy, and acceptable use, shall be documented, communicated periodically to responsible personnel, and reviewed at least annually to ensure continued relevance and effectiveness.

7. Human Resources Security

- Background verification of all employees having access to confidential data that includes verification of criminal records, previous employment records if any, and educational background.
- Signing of confidentiality agreement and acceptable use policy by employees upon their employment with clauses on protection of confidential information.
- Training on security and privacy awareness including training on PITS's policies, standards and relevant technologies along with maintenance and retention of training completion records.
- Employees will be required to adhere to the information security policies and procedures. Disciplinary process for non adherence will be defined and communicated.

8. Identity and Access management of PITS Personnel

- The Service Provider shall establish and maintain formal policies and procedures governing identity and access management, aligned to recognized standards such as ISO/IEC 27001 and NIST SP 800-63B.
- IAM controls shall enforce individual user accountability, role-based access, and principles of least privilege across systems that process or store Client Data.
- Access provisioning, modification, and de-provisioning shall follow documented workflows with appropriate authorization, traceability, and timely execution.
- Compliance with IAM requirements shall be reviewed periodically through internal audits or control assessments to ensure continued effectiveness and

adherence to regulatory and contractual obligations.

9. **Asset Management**

- The Service Provider shall establish and maintain an asset management framework that governs the lifecycle of information processing assets, including acquisition, classification, usage, and disposal, in accordance with recognized standards such as ISO/IEC 27001 and NIST CSF.
- All assets supporting service delivery shall be inventoried and assigned ownership, with documented policies defining acceptable use and responsibilities.
- Capacity planning and resource utilization shall be governed by formal policies to ensure scalability, performance, and alignment with business requirements.
- Secure disposal and reuse of electronic media and devices shall follow industry best practices to ensure data is rendered irrecoverable and that disposal activities are conducted through authorized channels.

10. Physical Security

- The Service Provider shall implement and maintain physical access control policies and procedures to safeguard facilities housing information systems and Client Data, in alignment with recognized standards such as ISO/IEC 27001 and NIST SP 800-53.
- Access to data centers, development environments, and other restricted areas shall be governed by formal approval workflows and enforced through secure mechanisms including electronic access controls, multi-factor authentication, and surveillance systems.
- Visitor access shall be managed through documented authorization procedures, with access records maintained and reviewed periodically.
- Physical access rights will be limited to authorized personals only and access shall be revoked promptly upon termination of employment, role change, or access expiry, and subject to periodic review to ensure continued appropriateness.

11. Network Security and Operations

- The Service Provider shall maintain a dedicated Network Operations Center (NOC) to oversee infrastructure health and availability through continuous monitoring and alerting mechanisms.

- Network security controls, including firewall configurations and segmentation policies, shall be implemented and maintained in accordance with documented security requirements and business justifications. These controls shall be reviewed periodically to ensure continued relevance and effectiveness.
- Logical separation of production, development, and integration environments shall be enforced to prevent unauthorized access and ensure that production data is not replicated or used in non-production systems.
- Access to production environments shall be governed by centralized identity management systems and protected through strong authentication mechanisms, including multi-factor authentication and encrypted credentials.
- Distributed Denial of Service (DDoS) mitigation capabilities shall be deployed using reputable service providers to ensure service resilience and availability.

12. Secure Software Development and Change Governance

- The Service Provider shall maintain a secure software development lifecycle (SDLC) framework that integrates security and privacy considerations throughout all phases of product design, development, testing, and deployment.
- Formal change and release management policies shall be implemented to ensure that modifications to systems, applications, or infrastructure are authorized, tested, and deployed in a controlled and auditable manner, minimizing disruption and risk.
- The Service Provider shall maintain governance measures to assess and manage risks associated with third-party software components, including licensing, security vulnerabilities, and version control, in alignment with recognized standards such as ISO/IEC 27001 and NIST.
- All development and deployment activities shall be subject to periodic review to validate the effectiveness of controls and ensure continued alignment with contractual, regulatory, and operational requirements.

13. Data Security and Management

- The Service Provider shall maintain a documented data classification and handling framework that governs access control, storage, and transmission of Client Data, in accordance with applicable legal and regulatory requirements.
- Logical separation of Client Data shall be enforced across all service environments to ensure data isolation and prevent unauthorized access

between subscribers**.**

14.Cryptography

- The Service Provider shall implement cryptographic controls to protect data in transit and at rest, using encryption protocols and key management practices aligned with recognized standards such as ISO/IEC 27002 and NIST SP 800-57.
- Transport encryption shall be applied to all data traversing networks outside the Service Provider's direct control, including public and wireless networks.
- Sensitive data at rest shall be encrypted using strong algorithms and key lengths appropriate to the data type and business context.
- Passwords shall be stored using secure, industry-recognized hashing algorithms and managed through cloud-native services such as Azure Key Vault or AWS Secrets Manager, which provide secure credential storage and access control.
- Encryption keys shall be managed through dedicated cloud-based Key Management Services (KMS), including Azure Key Vault and AWS KMS, with layered protection such as encryption of data keys using master keys and strict access controls.
- Master keys and data encryption keys shall be logically and physically separated, and subject to periodic review and rotation in accordance with the Service Provider's security policies.

15.Configuration Management

- The Service Provider shall maintain a documented configuration management policy that governs the establishment, maintenance, and review of baseline configurations for systems supporting service delivery.
- Baseline configuration standards shall be aligned with recognized industry frameworks, including the CIS Benchmarks (Level 1 or Level 2 profiles, as applicable), and shall be reviewed periodically to ensure continued relevance, security, and compliance.
- System configurations shall incorporate security hardening principles, including the removal of non-essential components and enforcement of secure default settings, in accordance with approved baseline definitions.
- Installation and modification of software components within production

environments shall be subject to formal approval processes and change control procedures, ensuring traceability and alignment with the Service Provider's governance framework.

16.Vulnerability Management

- The Service Provider shall maintain a documented vulnerability management policy that governs the identification, assessment, prioritization, and remediation of security vulnerabilities across systems and applications supporting service delivery.
- Vulnerability assessments and penetration testing shall be conducted periodically in accordance with recognized industry standards and methodologies, with remediation timelines aligned to the severity and contractual service levels.
- The Service Provider shall monitor authoritative threat intelligence sources and vulnerability databases (e.g., OWASP, CVE, NVD) to ensure timely awareness and response to emerging risks.
- Remediation of identified vulnerabilities shall be prioritized based on risk classification and tracked through formal processes to ensure timely resolution and compliance with applicable obligations.
- Endpoint protection and malware defense shall be governed by documented policies that ensure the use of current, industry-standard security controls and update mechanisms**.**

17.Security Logging and Monitoring

- Logging mechanisms shall be implemented to capture and correlate events from infrastructure, applications, and network components, supporting timely detection and investigation of security incidents.
- A centralized Security Information and Event Management (SIEM) platform shall be utilized to aggregate, normalize, and analyze log data, enabling threat detection, anomaly identification, and forensic investigation capabilities.
- Audit logs shall record privileged access, authentication attempts, system anomalies, and other information security events, and shall be retained in accordance with applicable legal, regulatory, and contractual requirements.
- Access to log data shall be restricted to authorized personnel, with safeguards in place to ensure confidentiality, integrity, and availability of log information.

- Intrusion detection and monitoring capabilities shall be maintained to support proactive threat identification and incident response, including integration with SIEM and other security analytics tools.

18.Business continuity and Disaster recovery

- The Service Provider shall maintain documented disaster recovery (DR) and business continuity (BC) policies and procedures designed to ensure the continuous availability of services and effective recovery in the event of a disruption.
- Business continuity plans shall be reviewed at least annually to assess their adequacy, effectiveness, and alignment with operational, contractual, and regulatory requirements.
- Redundancy mechanisms shall be implemented to eliminate single points of failure, including resilient infrastructure components and near real-time replication of application data across geographically separated data centers.
- Backup policies shall govern the periodic creation, encryption, and secure storage of system and application data, with retention periods of three (3) months and recovery testing conducted at defined intervals to validate restoration capabilities.
- The Service Provider shall commit to a minimum monthly service availability excluding scheduled maintenance and force majeure events.

19.Incident Management

- The Service Provider shall maintain a documented incident response policy and program that defines procedures for identifying, reporting, assessing, and responding to information security incidents in a timely and effective manner.
- Security incidents shall be tracked and managed through formal processes, including root cause analysis, corrective actions, and preventive controls to reduce recurrence risk.
- Incident notification procedures shall be established to ensure timely communication with Clients and relevant stakeholders, in accordance with contractual and regulatory breach reporting obligations.

REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK

Exhibit E

PRIVACY TERMS

In the course of providing PITS Services under the Agreement, PITS and its affiliated group entities ("PITS") may process Personal Information on behalf of the Subscriber. Accordingly, the parties agree as follows:

1. Interpretation

1.1 “Data Subject” means the individual who is identifiable by the Personal Information or to whom the Personal Information otherwise pertains;

1.2 "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information; and

1.3 "Personal Information" means any information relating to an identified or identifiable natural person that is provided to PITS by, or on behalf of, Subscriber through Subscriber’s use of the PITS Services.

Capitalized terms used but not defined in this Privacy Terms will have the meanings provided in the Agreement.

2. Processing of Personal Information

2.1 PITS shall process the Personal Information only on behalf of the Subscriber and in compliance with its instructions, unless otherwise required by applicable laws. Subscriber agrees that its instructions to PITS for processing Personal Information are:

(i) to process such data strictly in accordance with the Agreement;

(ii) to process data where such processing is initiated by Subscriber via the user interface of the PITS Services;

(iii) to process data for fraud prevention, spam filtering, and service improvement,including automation; and

(iv) to process data to comply with other documented reasonable instructions provided by Subscriber (eg., via email) where such instructions are consistent with the Agreement. PITS shall not be obliged to act in accordance with any instructions outside the scope of the Agreement except with the prior written agreement of both parties.

3. Service Providers

3.1 Subscriber understands that PITS engages sub-processors and third party service providers listed by PITS in its websites for providing (a) specific functionalities of PITS Services and (b) certain essential functions such as fraud detection, spam filtering and improvement of services (collectively "Service Providers") and that certain data, including Personal Information, may be shared by PITS to the Service Providers or may be collected by Service Providers in the process of providing such functionalities.

3.2 If Subscriber requests PITS for information on data processing by Service Providers,

such as for conducting a data protection impact assessment, PITS shall make commercially reasonable efforts to provide relevant information to Subscriber.

3.3 PITS warrants that it (i) publishes and maintains a list of Service Providers on its website; and (ii) will inform Subscriber prior to appointment of any new Service Provider.

3.4 Upon notification regarding PITS's intention to engage a new Service Provider, Subscriber may, within 10 days, object to the appointment of such new Service Provider by notifying PITS. In the event Subscriber objects to appointment of a new Service Provider, PITS shall recommend to the Subscriber, to the extent feasible, commercially reasonable changes in the configuration or use of the PITS Services to avoid data collection or processing by the Service Provider ("Reasonable Alternative"). If PITS is unable to provide Subscriber with a Reasonable Alternative, Subscriber may, upon written notice to PITS, terminate use of PITS Services and be entitled to full refund of subscription fee for unused portion of the subscription period.

4. Data Subject Requests

4.1 PITS shall promptly notify the Subscriber about any request received directly from the Data Subject without responding to that request unless it has been otherwise authorized to do so. Subscriber hereby agrees that PITS is authorized to respond in the first instance to any request in order to determine if the request is in respect of

Personal Information processed by PITS on behalf of the Subscriber.

4.2 PITS shall implement appropriate technical and organizational measures to enable the Subscriber to comply with Data Subject's requests to Subscriber to delete, rectify, access, or restrict processing Data Subject's data. Where Subscriber requests PITS's assistance under this section and PITS has already enabled Subscriber to comply with such requests by implementing appropriate technical and organizational measures, PITS shall have the right to charge the Subscriber for any reasonable costs or expenses incurred by PITS in order to assist Subscriber with request(s) from Data Subjects.

5. Confidentiality and Security

5.1 PITS shall ensure that its personnel engaged in the processing of Personal Information are (i) informed of the confidential nature of the Personal Information; and (ii) subject to confidentiality obligation or professional or statutory obligations of confidentiality.

5.2 PITS shall implement appropriate technical and organisational security measures as specified under Exhibit D to protect the Personal Information against any Security Incident.

6. Breach Notification

6.1 PITS shall notify Subscriber without undue delay after becoming aware of any Security Incident. PITS shall take all commercially reasonable efforts to remediate the Security Incident and prevent recurrence. PITS's obligation specified herein shall not apply to Security Incidents caused by Subscriber or its authorized users.

7. Audit

7.1 PITS shall, upon request by Subscriber, demonstrate its compliance with this Privacy Terms or Exhibit – D by way of reports of audits conducted in the previous 12 months by qualified and independent third party auditors. Subscriber acknowledges that all documents and information disclosed by PITS ("Audit Information") constitute PITS's confidential information. Accordingly, Subscriber shall take reasonable measures to protect the confidentiality of the Audit Information from unauthorized access, use or disclosure. Subscriber may use the audit reports only for the

purposes of meeting its regulatory audit requirements or confirming compliance with the requirements of this Privacy Terms by PITS.

7.2 Where the information provided by PITS under above clause is not sufficient to demonstrate compliance with Privacy Terms or Exhibit - D, Subscriber may request PITS for further information or audit of PITS's data processing facilities. Subscriber agrees that any audit of PITS's data processing facilities will be subject to an audit plan mutually agreed upon by both parties.

8. Return and Deletion Upon Termination

8.1 PITS shall provide an option to Subscriber to export Personal Information via the user interface of the PITS Services.

8.2 Upon termination or expiration of PITS Services, unless required by applicable law, Personal Information shall be automatically deleted from PITS's primary servers on completion of the next routine clean-up cycle (that occurs once in six months) and from its

backups after 3 months of deletion from primary servers.

8.3 Upon the request of the Subscriber, PITS shall provide confirmation of the completion of the relevant clean-up cycle as certification of destruction of the Personal Information.

REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK