

PLEASE REVIEW THESE PATHWAY TERMS OF SERVICE CAREFULLY. ONCE ACCEPTED, THESE PATHWAY TERMS OF SERVICE BECOME A BINDING LEGAL COMMITMENT BETWEEN YOU AND PATHWAY. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, YOU SHOULD NOT ACCEPT THIS AGREEMENT, CREATE AN ACCOUNT, OR USE PATHWAY'S SERVICES OR SOFTWARE.

*Notwithstanding anything to the contrary, if you have a separate written agreement with Pathway for your use of the Software, these Pathway Terms of Service will not apply to you, unless that written agreement does not cover a particular Software, in which case, these Pathway Terms of Service apply solely to your use of that particular Software.*

These Pathway Terms of Service, in combination with the terms of the sign up process (the “**Purchase Order**” or “**PO**”) on the Platform (as defined below), collectively form the contract (the “**Agreement**”) and set forth the terms for your use of the Software and Platform (as defined below) and are effective as of the date you accept or otherwise agree to the terms of this Agreement (“**Effective Date**”). This Agreement is between Iterro Inc. operating as Pathway (“**Pathway**”) and you or the organization on whose behalf you are accepting or otherwise agreeing to the terms of this Agreement (hereinafter, the “**Client**” or “**you**”/”**your**”).

Pathway may update the terms of this Agreement from time to time. Pathway will provide you with written notice of any material updates at least thirty (30) days prior to the date the updated version of this Agreement is effective, unless such material updates result from changes in laws, regulations, or requirements from telecommunications providers. Notices for material updates to the terms of this Agreement will be given to you. Following such notice, your continued use of the Software and/or Platform on or after the date the updated version of this Agreement is effective and binding, as indicated at the top of this Agreement, constitutes your acceptance of the updated version of this Agreement. The updated version of this Agreement supersedes all prior versions. If you do not agree to the updated version of this Agreement, you must stop using the Software and/or Platform immediately.

If you are the party that agreed to the terms of this Agreement and you reassign its account to a third-party reseller for administration purposes, such account reassignment will not excuse your obligations under this Agreement. Your use of the Software will continue to be subject to this Agreement.

**WHEREAS**, Pathway wishes to license the use of certain Automated Client Management System Software, including Renewal Automation, Marketing Automation, Staying-N-Touch, Self-Service Kiosk, Self-Service Kiosk widget and/or StormVision (collectively or individually the “**Software**”) as being accessed by individual user or the end-user (the “**Authorized Users**”) through the Pathway platform (the

“Platform”), including any updates, modifications, revisions, and third party products or services designed to interoperate with the Software.

**AND WHEREAS**, Client desires to use the Software from Pathway made available through the Platform.

**NOW THEREFORE**, the parties hereto (the “**Parties**”) agree as follows:

**1. Effective Date.**

This Agreement shall be effective as of the Effective Date and shall remain in effect until otherwise terminated in accordance with the provisions of the Agreement outlined herein.

**2. Selected Software and License Grants.**

**a.** Subject to Client’s compliance with the terms, conditions and restrictions as set forth in this Agreement, Pathway grants Client, and its limited number of Authorized Users (as defined in the PO) a limited, non-transferable, and non-exclusive license to use those elements of the Software made available for use by Pathway and as identified in the PO as the selected Software (the “**Selected Software**”), solely in machine-readable form, and solely for Client’s business of being an insurance broker, which shall include procuring and/or renewing insurance policies, for the limited use of the Authorized Users.

**b.** The Client agrees to ensure that all individuals accessing the Software, are employees or contractors, do so under authorized use by the Client, access such within Client’s premises or on hardware owned/leased by the Client, and will ensure its Authorized Users compliance with the Authorized Users Terms of Use. The Client shall not provide their access code or password to any third parties and any unauthorized access granted by Client or as a result of the Client’s actions are the responsibility of the Client. The Client acknowledges and agrees that the only the number of users as disclosed to Pathway shall be permitted to access the Software. Pathway reserves the right to audit the Client for their compliance with the terms of this Agreement.

**c.** Upon full payment of Fees, Pathway grants Client ownership of any extracted reports from the Selected Software, which Company may download, copy, distribute, modify and create derivative works of, subject to Pathway retaining ownership of all underlying Intellectual Property Rights in the reports.

**d.** Subject to the limited rights expressly granted hereunder, Pathway reserves all rights, title and interest in and to the Platform and the Software, Pathway’s Confidential Information, and any feedback or suggestions Client or its Authorized Users provide regarding the Software or Platform, including all related Intellectual Property Rights. No rights are granted to Client hereunder other than as expressly set forth herein. For the purposes of this Agreement, “**Intellectual Property Rights**” means all patents (including all reissues, divisions, continuations, and extensions thereof) and patent applications, trade names, trademarks, service marks, logos, trade dress, copyrights, trade secrets, mask works, rights in technology, know-how, rights in content (including performance and synchronization rights), unregistered design, or other intellectual property rights that are in each case protected under the laws of any governmental authority, whether or not registered, and all applications, renewals and extensions of the

same, but exclusive of any confidential or proprietary information, trade secrets, or intellectual property of Client.

e. Client acknowledges that the features and functions of the Software may change over time; provided, however, Pathway will not materially decrease the overall functionality of the Software.

### **3. Restrictions on Use.**

Except as otherwise expressly permitted under this Agreement, Client is not authorized to: (a) reverse engineer or otherwise attempt to discover the source code of or trade secrets embodied in the Software or any portion thereof; (b) distribute, transfer, sublicense to, or otherwise make available the Software (or any portion thereof) to third parties, including, but not limited to, making the Software available (i) through resellers or other distributors; or (ii) as an application service provider, service bureau, or rental source; (c) create modifications to or derivative works of the Software or the content contained therein; (d) attempt to modify, alter, or circumvent the licence control and protection mechanisms within the Software; (e) use any information or articles including but not limited to, the newsletters outside of the Software, such as use on the Client's own website; or (f) use or transmit the Software in violation of any applicable law, rule or regulation, including any data privacy laws or anti-spam laws.

Suspension of Services. Pathway may suspend its services to Client immediately upon written notice to Client for cause if Pathway, in good faith, determines: (a) that Client or its Authorized Users materially breach (or Pathway, in good faith, believes that Client or its Authorized Users have materially breached) any provision of this Agreement (including schedules hereto) or PO; (b) there is an unusual and material spike or increase in Client's use of the Software and that such traffic or use is fraudulent or materially and negatively impacting the operating capability of the Software; (c) that its provision of the Software is prohibited by applicable law or regulation; (d) there is any use of the Software by Client or its Authorized Users that threatens the security, integrity, or availability of the Software; or (e) that information in Client's account is untrue, inaccurate, or incomplete. In any of these case, Client shall still remain responsible for the Fees.

In this paragraph, "**spam**" includes one or more unsolicited commercial electronic messages to which Canada's anti-spam legislation ("**CASL**") or similar legislation applies, and derivations of the word "Spam" have corresponding meanings. Pathway may immediately terminate any account that it determines, in its sole discretion, is transmitting or is otherwise connected with any "spam" or other unsolicited bulk email. In addition, if actual damages cannot be reasonably calculated, Client agrees to pay Pathway liquidated damages of five dollars (U.S. \$5.00) for each piece of "spam" or unsolicited bulk email transmitted from or otherwise connected with Client's account or its users accounts. Otherwise, Client agrees to pay, and agrees to indemnify and hold Pathway harmless, for Pathway's actual damages or penalties to the extent such actual damages can be reasonably calculated. Pathway reserves the right to

block, reject, or remove what it considers to be "spam" or other unsolicited bulk email from the Software and/or Platform and Pathway shall have no liability for blocking any email considered to be "spam."

#### **4. Licenses by Client.**

**a.** Client grants Pathway a limited-term license to copy, access, transmit and display the electronic data and information submitted by or for Client to the Software or collected and processed by or for Client using the Software ("**Client's Data**") for purposes set forth hereunder and otherwise generally for Pathway to provide the services contracted for hereunder. Pathway acquires no right, title or interest from Client under this Agreement in or to Client's Data.

**b.** By using any third party software, feature or widget on Pathway's website, Client, on its behalf and on behalf of its users, hereby authorizes Pathway to share such Client's Data, as has been provided by the Client or its user(s) in their use of the third party software, feature or widget, with such third party service provider. Client and/or its users hereby agree to have read and accept the third party's terms and conditions as they apply to the Client and/or its users' use of such third party services.

**c.** Further, if the Selected Software is to be provided in the brand of the Client, the Client hereby provides its consent for Pathway to use and display the logo, name and other branding particulars of the Client (collectively, "**Client Marks**") on all messages, articles, reminders and campaigns provided by the Selected Software. The Client hereby warrants that the Client has all authority and control over the selected branding elements, including the Client's logo to permit the licensing contemplated herein.

**d.** Notwithstanding anything in this Agreement to the contrary, Client authorizes Pathway to use deidentified and non-personal Client's Data disclosed through Platform or Software usage or other data collection activities for product development purposes.

**e.** So long as the Client remains a customer and/or client of Pathway, Client shall be deemed to have granted Pathway a license to use the Client Marks for Pathway's marketing, research, business development and advertising purposes, including without limitation, in the emails, newsletters, marketing and advertising communications, social media, blog posts, website of Pathway.

**f.** Pathway's use of the Client Marks is a non-exclusive, non-transferable, revocable, limited license to use the Client Marks in accordance with the terms hereof. Any use of the Client Marks will not contain libelous, defamatory, obscene, abusive or otherwise unlawful material or material that infringes the rights of third parties, or material that disparages Client or otherwise impairs the goodwill associated with either Client or the Client Marks. Pathway further acknowledges Client's exclusive rights in and to the Client Marks and the goodwill pertaining thereto. Pathway acknowledges that it has no right, title, license, or interest, express or implied, in and to the Client Marks, except for the limited license specifically provided in this Agreement. Pathway agrees that it shall not challenge or contest the validity of the Marks or Client's ownership thereof or the validity of this Agreement, or engage in any act or assistance to any act which may infringe or lead to the infringement of any of the Client Marks. Pathway will use commercially reasonable efforts to comply with all reasonable Client Mark usage guidelines that Client may communicate in writing from time to time. Client reserves the right to audit the use of the Client Marks

by Pathway upon reasonable prior written notice and in any reasonable manner, and Pathway agrees to provide Client with copies of any materials or other documents reasonably requested by Client in association with any such audit.

**5. Delivery.**

The Selected Software is delivered electronically, and delivery is deemed effective on the later of the Effective Date or the date that the applicable Fees are paid in full.

**6. Pathway's Obligations.**

Pathway shall during the Term of this Agreement :

- a) provide Client with timely support for the Selected Software, during regular business hours, at no additional cost to Client;
- b) employ reasonable efforts to ensure the Selected Software is available for use at minimum 99 percent of the time; and
- c) arrange, to the extent possible, for scheduled maintenance outside regular office hours.

Pathway shall comply with the Support Services and Service Levels set forth in **Schedule A**.

**7. Responsibility for Data.**

The Client acknowledges that the source data used by Pathway within the Platform, the Renewal Automation, Marketing Automation, Staying-N-Touch, Self-Service Kiosk, Self-Service Kiosk widget and/or StormVision software relies upon the Client providing access to accurate information in relation to their existing, former and/or potential clients. Pathway shall not independently verify, nor shall Pathway be responsible for the dissemination of inaccurate information through the Software, including without limitation information regarding effective insurance dates or renewal information, which was not accurate at the source, being the Client's BMS. Client shall at all times be responsible for all information which is sent to the Client's clients which is derived from the Clients information or the Client's BMS, and the Client shall be liable, and hereby agrees to indemnify and hold Pathway harmless, for any losses or damages suffered by either the Client or Pathway as a result thereof.

The Client hereby confirms that the Client has obtained any and all consents from any of the Client's clients or potential clients that would allow for the Client to provide the Client's clients' non-public information to Pathway, which may be required or used in the provision of the services offered by the Selected Software. Pathway shall not be responsible for any obligations in regards to non-public information not otherwise agreed to within this Agreement, the Pathway's Privacy and Security Policy and their Terms of Use, which are accessible on Pathway's website, being [www.pathwayport.com](http://www.pathwayport.com). By agreeing to this Agreement, the Client confirms that he/she has read and accepts the terms contained within both the Privacy and Security Policy and the Terms of Use. Similarly, Pathway takes no responsibility for

any inaccuracies or failures to report any weather-related event within any alerts or updates as contemplated by the StormVision Software. Although Pathway makes every effort to verify the contents of the newsletter and informational articles contained within the Software, Pathway does not provide any warranty or confirmation about the accuracy of the information, nor should the information be considered to be a replacement of insurance, accounting or legal advice.

Pathway shall comply with the Data Security Standards set forth in **Schedule B**.

#### **8. Fees.**

The Client shall be responsible for the fees associated with the Selected Software as outlined within the PO (the “**Fees**”). If the Client uses any Software not set forth in the applicable PO, the Client will be charged the then applicable rates listed on Pathway’s website.

Fees are invoiced monthly and due in advance, each month of the Term on the day in which the Client first signed up for the Selected Software, via credit card for the Selected Software active for that month. Except as otherwise expressly set forth herein, payment obligations are non-cancelable and once paid, no refund or rebate shall be provided in the event that a Selected Software is cancelled at any time during the Term.

If Client’s account does not have sufficient funds or its credit card declines a charge for the Fees due, Pathway may suspend the provision of its services to all of Client’s accounts until the Fees due are paid in full. Client is prohibited from creating new accounts until the Fees due are paid in full.

All fees are exclusive of any applicable taxes, levies, duties, or other similar exactions imposed by a legal, governmental, or regulatory authority in any applicable jurisdiction, including, without limitation, sales, use, value-added, consumption, communications, or withholding taxes (collectively, “**Taxes**”). Client will pay all Taxes associated with this Agreement, excluding any taxes based on Pathway’s net income, property, or employees. If Client is required by applicable law to withhold any Taxes from payments owed to Pathway, Client will reduce or eliminate such withheld Taxes upon receipt of the appropriate tax certificate or document provided by Pathway. Client will provide Pathway with proof of payment of any withheld Taxes to the appropriate authority.

#### **9. Confidentiality Obligations**

For the purposes of this Agreement, “**Confidential Information**” means any information disclosed, in any format, by one party (the “**Disclosing Party**”) to the other party (the “**Receiving Party**”) relating directly or indirectly to but is not limited to prototypes, trade secrets, intellectual property, information, technical data, research, products, software, services, development, macros, source code, unreleased software, inventions, ideas, processes, designs, drawings, engineering, marketing, markets, Personal

Information, business plans, business policies or practices, forecasts or financial information, team process, design process, part supply, pricing, development process and procedures, disclosed by the Disclosing Party to the Receiving Party under this Agreement which at the time of disclosure is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the parties, exercising reasonable business judgment, to be confidential. Confidential Information shall include, but not be limited to, all materials marked as confidential information. The Confidential Information shall at all times remain the sole property of the Disclosing Party, and shall include any partial, and derivative information, insofar as the same are and remain Confidential Information of the Disclosing Party not generally known or available to the public, through no actions of the Receiving Party.

For purposes hereof, “**Permitted Parties**” means those employees, accountant’s and legal advisors of the Receiving Party for whom the confidential Information must be disclosed in the evaluation of the Purpose.

All disclosures of Confidential Information (whether written or oral) by either party shall (a) remain in confidence until the later of i) three (3) years from the date of disclosure, or ii) the expiry of this Agreement, save and except that any trade secrets or information with respect to the Disclosing Party’s products and/or research and development which shall remain confidential in perpetuity; (b) be disclosed only to Permitted Parties who are bound by obligations of confidentiality in favour of the Receiving Party with terms similar to or stronger than those contained herein; and (c) be reproduced or used by the Receiving Party only to the extent necessary for the offering or use of the Selected Software. The Receiving Party shall protect the Confidential Information with the same degree of care as it normally exercises to protect its own confidential information of similar nature, but at a minimum with a reasonable degree of care to prevent its unauthorized use, dissemination or publication. The Receiving Party pledges and agrees that it shall keep confidential any and all of the Confidential Information and other such matters arising hereto, and shall not disclose to any other person or persons, corporation, agent or consultant with whom it is or may be associated with, any Confidential Information without the express written permission of authorized officer of the Disclosing Party. The Receiving Party agrees to advise the Disclosing Party immediately in the event of an inadvertent or accidental disclosure of the Confidential Information or in the event of an electronic system breach.

All materials, including Confidential Information disclosed by the Disclosing Party under this Agreement shall remain the property of the Disclosing Party. Each party shall, upon the completion of this Agreement or at the request by the Disclosing Party, return all materials received or obtained under this Agreement, including Confidential Information, and all copies and all documents containing any portion of any Confidential Information, including a deletion of all electronic copies, including any back-up copies. Notwithstanding anything to the contrary contained above, the Confidential Information may be disclosed to the extent that such disclosure is necessary to comply with any law, regulation, or order of court,

provided that the Receiving Party shall give the Disclosing Party reasonable advance notice of any such proposed disclosure (as legally permissible), and shall use its reasonable best efforts to secure an agreement in writing to be bound by the provisions of this Section 9 from any person obtaining access to the Confidential Information pursuant to this Section 9. The Receiving Party shall advise the Disclosing Party in writing of the manner of such disclosure. Information shall be deemed not to be confidential if such information is or becomes publicly known through no wrongful act of the Receiving Party, or is already known by the Receiving Party as evidenced by competent proof thereof, or is approved for release by the prior written approval of the Disclosing Party, or is rightfully received by the receiving party from a third party without restriction and without breach of this agreement, or is disclosed by the Disclosing Party to a third party without a similar restriction on the rights of such third party, or is independently developed by the receiving party without the use of the Confidential Information.

**10. General Obligations.**

**a.** The Parties acknowledge and agree to comply with all applicable legal obligations relating to the privacy, security, integrity, and confidentiality of all data and information used by the Software which enables identification of the retail or individual customer(s) (“**Personal Information**”). The Parties further agree to collect, use and disclose Personal Information in accordance with the Personal Information Protection and Electronic Documents Act of Canada (“**PIPEDA**”), and all applicable laws governing the protection of personal information;

**b.** Each Party shall, at a minimum, implement and maintain appropriate administrative, technical, and physical safeguards reasonably designed to: (i) ensure against any anticipated threats or hazards to the security or integrity of the Personal Information; and (ii) protect against unauthorized access to or use of the Personal Information; and

**c.** Each Party may disclose Personal Information, as required, pursuant to any federal or provincial laws, and/or regulations. These provisions shall apply during the Term and after the termination of this Agreement.

**d.** At all times, Client shall, and shall cause its users to, comply with their obligations under CASL or similar anti-spam legislation applicable to them. In the event of a breach thereof, Client agrees to indemnify and hold Pathway harmless from all damages, fines, losses and penalties incurred by Pathway as a result of such breach.

**11. Non-Solicitation.**

Each party agrees that, for a period of eighteen (18) months following ending of this Agreement, it shall not solicit to employ or enter a consulting arrangement with any of the officers, employees, directors or consultants of the other party which whom such party has had contact or were identified to such party in connection with the Software offered hereunder. The term “solicit to employ or enter into a consulting arrangement with” shall not be deemed to include generalized searches by the Client for employees or

consultants through media advertisements, employment firms or otherwise, that are not focused on persons employed by or who consult for Pathway.

**12. Remedies.**

Subject to the terms contained within this paragraph, both parties acknowledge that compliance with the provisions of this Agreement is necessary to protect their proprietary interests. Each party further acknowledges that any unauthorized use or disclosure to any person or entity in breach of this Agreement may result in irreparable and continuing damage, and that each party shall be authorized and entitled to seek immediate injunctive relief and any other rights or remedies to which it may be entitled. If either party violates any of the terms contained within this Agreement, it acknowledges that money damages will be an inadequate remedy and that the violated party will be entitled to specific performance or to injunctive relief to prohibit the violating party from continuing to violate this agreement even if no money damages can be proven.

**13. Representations and Warranties and Disclaimer.**

a. Each party represents and warrants that it has validly accepted or entered into this Agreement and has the legal power to do so.

b. Client represents and warrants that it has provided and will continue to provide adequate notices, and that it has obtained and will continue to obtain the necessary permissions and consents, to provide Client's Data to Pathway for processing.

c. WITHOUT LIMITING PATHWAY'S EXPRESS WARRANTIES AND OBLIGATIONS HEREUNDER, AND EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE SOFTWARE AND SERVICES ARE PROVIDED "AS IS," AND PATHWAY MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT TO THE FULLEST EXTENT PERMITTED BY LAW. PATHWAY ADDITIONALLY DISCLAIMS ALL WARRANTIES RELATED TO TELECOMMUNICATIONS PROVIDERS' NETWORKS ARE INHERENTLY INSECURE AND THAT PATHWAY WILL HAVE NO LIABILITY FOR ANY CHANGES TO, INTERCEPTION OF, OR LOSS OF CUSTOMER DATA WHILE IN TRANSIT VIA THE INTERNET OR A TELECOMMUNICATIONS PROVIDER'S NETWORK. BETA OFFERINGS ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITH NO WARRANTIES AND PATHWAY WILL HAVE NO LIABILITY AND NO OBLIGATION TO INDEMNIFY FOR ANY BETA OFFERING WHATSOEVER.

**14. Limitation of Liability**

a. Neither party shall be liable for any of the following losses or damages (whether or not foreseen, indirect, foreseeable, known or otherwise): (i) loss of profits (whether actual or anticipated), (ii) loss of revenue, (iii) loss of contracts, (iv) loss of anticipated savings, (v) loss of business, (vi) loss of opportunity, (vii) loss of goodwill, or (viii) any indirect, special, incidental, consequential, cover, lost data, business interruption, or punitive damages, whether an action is in contract or tort and regardless of the theory of liability, even if a party or its affiliates have been advised of the possibility of such damages or if a party's or its affiliates' remedy otherwise fails of its essential purpose. The foregoing disclaimer will not apply to the extent prohibited by law.

b. Pathway's total aggregate liability arising out of or in connection with the performance or contemplated performance of the services hereunder (including without limitation under all Schedules hereto) (whether for tort (including negligence), breach of contract, breach of statutory duty or otherwise) shall in no event exceed the price paid or payable by Client to Pathway or its affiliates hereunder within the 12 month period immediately before the date of the event giving rise to Client's claim. The foregoing limitation shall not apply to any breach of Confidentiality.

c. Nothing contained in the Agreement shall exclude or limit either party's liability for: (i) fraud or fraudulent misrepresentation; or (ii) any other matter for which it would be prohibited by applicable law to limit or exclude or attempt to limit or exclude liability. In all such cases a party's liability shall be limited to the greatest extent permitted by applicable law.

d. Access to the Software delivered via online systems is dependent on third parties, such as internet service providers. Pathway will have no liability to Client for any losses Client suffers resulting directly or indirectly from: (i) failures of performance on the part of Pathway's internet service provider; (ii) failure of Client's equipment or those of Client's candidate(s) or third parties; (iii) reasons related to Pathway's provision of scheduled system upgrades or maintenance; (iv) any security breach of Pathway's system unless such breach is shown to be the result of Pathway's negligence; or (v) inability to access the Pathway online system in any one country due exclusively to Pathway's software or hardware for any period not exceeding (a) ten (10) consecutive hours or (b) an aggregate of more than twenty-four (24) hours in any calendar month.

## 15. **Indemnification.**

- a) **Indemnification by Pathway.** Pathway will defend Client, its affiliates, and each of their directors, officers, and employees (collectively, "**Client Indemnified Parties**") from and against any claim, demand, suit, or proceeding made or brought against a Client Indemnified Party by a third party alleging that Pathway's provision of the Selected Software infringes or misappropriates such third party's intellectual property rights ("**Pathway Indemnifiable Claim**"). Pathway will indemnify Client from any fines, penalties, damages, attorneys' fees, and costs awarded against a Client Indemnified Party or for settlement amounts approved by Pathway for a Pathway Indemnifiable Claim. If Pathway's provision of the Selected Software has become, or in Pathway's opinion is likely to become, the subject of any Pathway Indemnifiable Claim for third-party intellectual

property rights infringement or misappropriation, Pathway may at its option and expense: (a) procure the right to continue to provide the Selected Software as set forth herein; (b) modify the Selected Software to make them non-infringing; or (c) if the foregoing options are not reasonably practicable, terminate this Agreement, or, if applicable, terminate the Selected Software that is the subject of any Pathway Indemnifiable Claim for third-party intellectual property rights infringement or misappropriation, and refund to the Client any unused pre-paid Fees.

- b) Limitations. Pathway will have no liability or obligation under this Section 15 with respect to any Pathway Indemnifiable Claim arising out of (a) Client's use of the Software in breach of this Agreement; (b) the combination, operation, or use of the Software with other applications, portions of applications, products, or services where the Software would not by themselves be infringing; or (c) Software for which there is no charge.
- c) Indemnification by Client. Client will defend Pathway, its affiliates, and each of their directors, officers, and employees (collectively, "**Pathway Indemnified Parties**") from and against any claim, demand, suit, or proceeding made or brought against a Pathway Indemnified Party by a third party alleging or arising out of Client or its Authorized Users' (i) breach of this Agreement, (ii) provision of the Client's Data to Pathway, or (iii) use of the Selected Software or the Platform, or arising out of a Client Application, including, without limitation, any claims that a Client Application, or Client or its Authorized Users' use of a Client Application, infringes or misappropriates such third party's intellectual property rights (collectively, "**Client Indemnifiable Claims**"). Client will indemnify Pathway from any fines, penalties, damages, attorneys' fees, and costs awarded against a Pathway Indemnified Party or for settlement amounts that Client approves for a Client Indemnifiable Claim. For purposes hereof, "**Client Application**" means any software application or service that Client makes available to its Authorized Users that interfaces with the Selected Software or Platform.
- d) Conditions of Indemnification. As a condition of the foregoing indemnification obligations: (a) the indemnified party ("**Indemnified Party**") will promptly notify the indemnifying party ("**Indemnifying Party**") of any Client Indemnifiable Claim or Pathway Indemnifiable Claim (individually or collectively referred to herein as a "**Claim**") in writing; provided, however, that the failure to give prompt written notice will not relieve Indemnifying Party of its obligations hereunder, except to the extent that Indemnifying Party was actually and materially prejudiced by such failure; (b) Indemnifying Party will have the sole authority to defend or settle a Claim; and (c) Indemnified Party will reasonably cooperate with Indemnifying Party in connection with Indemnifying Party's activities hereunder, at Indemnifying Party's expense. Indemnified Party reserves the right, at its own expense, to participate in the defense of a Claim. Notwithstanding anything herein to the contrary, Indemnifying Party will not settle any Claim for which it has an obligation to indemnify under this Section 15 admitting liability or fault on behalf of Indemnified Party, nor create any obligation on behalf of Indemnified Party without Indemnified Party's prior written consent, which will not be unreasonably withheld, conditioned, or delayed.
- e) Exclusive Remedy. This Section 15 states Indemnifying Party's sole liability to, and Indemnified Party's exclusive remedy against, the other party for any third-party claims.

## 16. Termination.

This Agreement will commence on the Effective Date and continue until terminated in accordance with either of the following (“**Term**”):

- a) For Convenience. Either party may terminate this Agreement for convenience by providing the other party with at least forty-eight (48) hours prior written notice.
- b) Non-Payment of Fees. Pathway may terminate this Agreement immediately due to the non-payment by the Client of any Fees, or by the breach of any provisions of this Agreement by the Client.
- c) Insolvency. Subject to applicable law, either party may terminate this Agreement immediately by providing written notice in the event of the other party’s liquidation, commencement of dissolution proceedings, or any other proceeding relating to a receivership, failure to continue business, assignment for the benefit of creditors, or becoming the subject of bankruptcy.

Upon Termination for any reason, the Client will cease to have access to any of the information or services offered by the Software. Notwithstanding the termination of this Agreement, terms contained within Sections 2, 3, 4, 7, 9, 10, 11, 14, 15 and 17 shall survive the termination of this Agreement.

**17. Miscellaneous.**

- a) Assignment. Neither party hereto may assign or otherwise transfer this Agreement or any applicable PO, in whole or in part, whether by operation of law or otherwise, without the other party’s prior written consent (not to be unreasonably withheld or delayed). Notwithstanding the foregoing, Pathway may assign this Agreement or any applicable PO, in whole or in part, without consent to (a) a successor to all or part of its assets or business or (b) an affiliate. Any attempted assignment, delegation, or transfer by either party in violation hereof will be void. Subject to the foregoing, this Agreement and any applicable PO will be binding on the parties and their respective successors and permitted assigns.
- b) Relationship. Each party is an independent contractor in the performance of each and every part of this Agreement. Nothing in this Agreement is intended to create or will be construed as creating an employer-employee relationship or a partnership, agency, joint venture, or franchise. Each party will be solely responsible for all of its employees and agents and its labor costs and expenses arising in connection therewith and for any and all claims, liabilities, damages, or debts of any type whatsoever that may arise on account of its activities, or those of its employees and agents, in the performance of this Agreement. Neither party has the authority to commit the other party in any way and will not attempt to do so or imply that it has the right to do so.
- c) No Third-Party Beneficiaries. This Agreement does not confer any benefits on any third party (including Client’s Authorized Users or an affiliate) unless it expressly states that it does.
- d) Notices. Notices to Pathway will be provided via email to [INSERT EMAIL]. All notices to Client will be provided via email to the relevant contact(s) Client designates in its account.
- e) Governing Law. This Agreement will be governed by and interpreted according to the laws of Ontario and the federal laws of Canada applicable therein, without regard to conflicts of laws and principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement. Any action arising out of this Agreement will be instituted in the courts of the city of Toronto and the parties hereby consent to the non-exclusive jurisdiction of these courts.

- f) Dispute Resolution. In the event of any dispute, claim, or controversy in connection with this Agreement (other than for disputes, claims, or controversies related to the intellectual property of a party) (collectively, “**Disputes**”), each party’s representatives will, in good faith, attempt to resolve a Dispute. If the parties are unable to resolve a Dispute within thirty (30) days or within such other time period as the parties may agree in writing, then the parties may commence binding arbitration under the Ontario *Arbitration Act*. The parties will share equally the fees and expenses of the arbitrator. The arbitration will be conducted by a sole arbitrator mutually agreed to between the parties or, failing that, by the ADR Institute of Ontario under its then prevailing rules. Judgment on the award rendered by the arbitrator may be entered in any court of competent jurisdiction. The arbitrator will have the authority to grant specific performance or any other equitable or legal remedy, including provisional remedies. Each party will be responsible for its own incurred expenses arising out of any dispute resolution procedure. Any arbitration proceedings will take place in the English language in the City of Toronto.
- g) Force Majeure. No failure, delay, or default in performance of any obligation of a party will constitute an event of default or breach of this Agreement to the extent that such failure to perform, delay, or default arises out of a cause, existing or future, that is beyond the control and without negligence of such party, including action or inaction of governmental, civil or military authority, fire, strike, lockout, or other labor dispute, flood, terrorist act, war, riot, theft, earthquake, or other natural disaster (collectively, “**Force Majeure Events**”). The party affected by a Force Majeure Event will take all reasonable actions to minimize the consequences of any such event.
- h) Waiver. No failure or delay by either party in exercising any right or enforcing any provision under this Agreement will constitute a waiver of that right or provision, or any other provision.
- i) Headings. Titles and headings of sections of this Agreement are for convenience only and will not affect the construction of any provision of this Agreement.
- j) Severability. In the event that any provision of this Agreement is held by a court or other tribunal of competent jurisdiction to be unenforceable, such provision will be limited or eliminated to the minimum extent necessary to render such provision enforceable and, in any event, the remainder of this Agreement will continue in full force and effect.
- k) Entire Agreement. This Agreement (including all exhibits and attachments hereto) will constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous understandings, proposals, statements, sales materials, presentations, or non-disclosure or other agreements, whether oral or written. No oral or written information or advice given by Pathway, its agents, or its employees will create a warranty or in any way increase the scope of the warranties or obligations in this Agreement.

## SCHEDULE “A” – SUPPORT SERVICES DESCRIPTION & SERVICE LEVELS

### 1. Definitions

- a. “**Availability**” means the percentage of time that Pathway makes available the Software and Platform to the Client in a fully functional and responsible manner, in accordance with Schedule “B” and the Agreement.
- b. “**Downtime**” means the percentage of time that the Software and Platform are not made available to the Client for any reason outside of the Client’s control.
- c. “**Incident**” means any event that is not part of the standard operations and that causes or may cause, an interruption to or reduction in the availability of the Software and/or Platform.
- d. “**Planned Maintenance**” is the time, not exceeding 5 hours per month, outside of Business Hours, for which Pathway must provide the Client with at least 48 hours’ written notice or as much notice as reasonably possible where an emergency security patch must be deployed to protect Client Data.
- e. “**Response Time**” means the time elapsed between an Incident being reported (ticket created) and the Incident being acknowledged by Pathway Support Personnel to initiate Support Services.
- f. “**Workaround**” means a strategy, plan or technique used to overcome the causes(s) of an Incident.

### 2. Support Services

Pathway shall provide the Client and its Authorized Users Support Services through its online platform (SLACK) and by email and telephone. The Support Services will be available 24 hours a day, 7 days a week. The Support Services include all new releases, versions, updates, upgrade, corrections, fixes, modifications, customizations and improvements to the Software, Platform and Services made or owned by Pathway. If any Support Services are not performed with reasonable skill, care and diligence, Pathway shall re-perform the Services. Pathway will assign a dedicated Client Success Manager (CSM) to the Client’s account to assist in support including the setup of the Client’s first campaign launch. Pathway will provide a monthly value report so it can show the Client all the benefits that Pathway is providing as part of its Services and Support.

### 3. Incident Response and Resolution Time Service Levels

- a. Incident severity levels and Incident response and Resolution or Workaround Delivery time Service Levels are set out in the table below:

<b>Support Levels</b>			
<b>Severity Level</b>	<b>Severity 1</b>	<b>Severity 2</b>	<b>Severity 3</b>
<b>Definition</b>	Any Incident which renders the Software, Platform or Services unusable to the Client. These are Incidents related to the Software, Platform or Services for which there is no alternate solution available	Any Incident which has a significant impact on business production, however, the Client can continue business operations in a restricted manner. These are Incidents related to the components of the Software, Platform or Services which are being faced or encountered by	Any Incident which is user-specific and does not have a direct impact on business production. The Software, Platform or services are usable and the Incident causes only minor inconvenience.

		multiple users at the same time.	
Coverage	24x7 (24 hours per day, 7 days a week)	24x7 (24 hours per day, 7 days a week)	24x7 (24 hours per day, 7 days a week)
Response Time SLA	<b>2-hour</b> call-back or electronic reply	<b>4-hour</b> call-back or electronic reply	<b>48 hours</b> call-back or electronic reply
Incident Resolution or Workaround Delivery Procedure SLA	<ul style="list-style-type: none"> <li>● Pathway will take immediate steps toward resolving the Incident.</li> <li>● Pathway will work with the Client to address Severity 1 Incidents until a solution is available or a Workaround is provided no later than <b>24 hours</b> from notification of Incident</li> <li>● If a Workaround is provided, Pathway will downgrade the severity of the Incident with prior written approval from the Client to get a permanent fix in a reasonable mutually agreed to timeframe.</li> </ul>	<ul style="list-style-type: none"> <li>● Pathway will take immediate steps to address the Incident.</li> <li>● Pathway will work with the Client to address Severity 2 Incidents until a solution is available or a Workaround is provided no later than <b>48 hours</b> from notification of Incident.</li> <li>● If a Workaround is provided, Pathway will downgrade the severity of the Incident with prior written approval from the Client to get a permanent fix in a reasonable mutually agreed to timeframe.</li> </ul>	Pathway will research Severity 3 Incidents within 3 Business Days of the first Pathway response. Pathway will provide a plan and timeframe to the Client to address Severity 3 Incidents within <b>96 hours</b> from notification of Incident.
Allowable Service Level Failure (per month) for: a) Resolution Time and b) Incident Resolution or Workaround Delivery	a) 2 b) 1	a) 2 b) 1	a) 3 b) 2
Incident Response Service Level Credits	2% of annual Fees if Allowable Service Level Failure (per month) is exceeded.	1% of annual Fees if Allowable Service Level Failure (per month) is exceeded.	.05% of annual Fees if Allowable Service Level Failure (per month) is exceeded
Incident Resolution or Workaround Delivery Service Level Credits	5% of annual Fees if Allowable Service Level Failure (per month) is exceeded.	2% of annual Fees if Allowable Service Level Failure (per month) is exceeded.	.05% of annual Fees if Allowable Service Level Failure (per month) is exceeded

Pathway will respond to any report of an Incident and will provide a plan to resolve the Incident as soon as possible. Pathway will provide a monthly report of all Incidents and achievement of Service Level agreements as well as applicable Service Level Credits.

4. Escalation Levels

Each Party’s escalation levels to escalate Incidents that are not resolved with the resolution times specified in Section 3 above are set out in the table below:

<b>Severity</b>	<b>Timeline for Notification if Resolution Service not met</b>	<b>the Client Notification Contacts</b>	<b>Pathway Notification Contact</b>
Level 1	12 hours		
	16 hours		
	20 hours		
Level 2	24 hours		
	28 hours		
	32 hours		

5. Availability Service Level

**Calculation.** Service Level Availability is calculated by subtracting the percentage of Downtime which does not include any Planned Maintenance from 100%.

6. Availability Service Level Credits.

a. **Credit Calculation.** Service level Credits are dollar credits calculated against the prorated monthly Fees for the Software, Platform and Service as set out in the table below:

<b>Availability</b>	<b>Service Level Credit</b>
Less than 99.9%	5%
Less than 99.0%	10%
Less than 95.0%	20%

b. **Set Off or Payment.** Pathway will set off the Service Level Credits against the next invoice for the Software, Platform or Services. If the Agreement has been terminated and no set-off can be credited against a future invoice or if the Service Levels exceed amounts payable by the Client, Pathway shall pay the Client any balance of Service Level Credits within 45 days of the end of the month in which the applicable Service Level Credits are calculated.

7. Reporting.

Pathway shall report any Incident response and/or resolution Service Level failures to the Client and provide monthly reports of Service Level Availability attainment and applicable Service Level Credits.

## SCHEDULE “B” – DATA SECURITY STANDARDS

This Schedule B (Data Security Standards) (this “**Schedule**”) is subject to and incorporated by reference to the attached Terms of Service (the “**Agreement**”). To the extent of any conflict or inconsistency between the provisions in the body of this Agreement and this Schedule, the terms of this Schedule shall prevail. Under this Schedule, “Service Provider” shall refer to Iterro Inc. operating as Pathway and “Customer” shall refer to Client (as defined in the Agreement).

Customer requires that its suppliers, vendors and other business partners, including Service Provider, comply with these Data Security Standards with respect to any data or other information (collectively, “**Customer Data**”) that Customer or its personnel make available or accessible to Service Provider in the context of Service Provider’s business relationship with Customer. All capitalized terms and phrases used herein but not otherwise defined shall have the same meanings set forth in the Agreement. This Schedule will survive termination of the Agreement for as long as Service Provider has Customer Data in its possession or under its control. Service Provider covenants, at Service Provider’s expense except where otherwise provided, the following:

### 1. Definitions.

1.1. “*Customer Data*” means (i) all information provided by Customer to Service Provider to enable the provision of access to, and use of, the services under the Agreement ; (ii) all content, data and information processed, recorded and stored for Customer in connection with Customer’s use of the Services; and (iii) Customer specific configurations and rules implemented in the Services. “Customer Data” includes, without limitation, any personally identifiable information or data concerning or relating to Customer’s employees, agents, customers or other individuals that Customer has dealings with, that may be used to uniquely identify or contact such employees, agents, customers or individuals, including commonly understood sub-categories such as Personal Sensitive Information (PSI), Protected Health Information (PHI), Personal Card Data (PCI), Personal Identity Information (PII), and other personal information or personal data as defined under applicable regulatory privacy regulations and regulated and confidential information, and Personal Information as defined under the Agreement.

1.2. “*Good Industry Practice*” means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances seeking to meet its obligations to the fullest extent possible.

1.3. “*Personnel*” means Services Provider’s employees, contractors, suppliers, subcontractors (other than Excepted Subcontractors, as defined below) and any other persons who have access to Service Provider’s facilities, systems, or Customer Data.

2. Security Program Requirements. Service Provider shall establish and maintain a comprehensive “Security Program” that has the physical, administrative, and technical safeguards to: (i) ensure the integrity, security and confidentiality of Customer Data; (ii) protect against threats and hazards to the security of Customer Data, and (iii) protect against any loss, misuse, unauthorized, accidental or unlawful access, disclosure, alteration and destruction of Customer Data. All of the foregoing shall be no less rigorous than those maintained by Service Provider for its own data and information of a similar nature; and shall ensure compliance with the provisions of applicable law

---

---

## PATHWAY TERMS AND CONDITIONS

---

and regulations and Good Industry Practice. Upon request, Service Provider shall provide Customer appropriate documentation evidencing compliance with these requirements. Such measures will include implementing and maintaining the following which Service Provider will be responsible for ensuring are maintained at all times by it and its Personnel:

2.1. Physical Security Measures

(a) Physical Data. Service Provider shall not keep any Customer Data in physical form unless required as part of providing the Services and is authorized by Customer.

2.2. Administrative Security Measures

(a) Background Checks and Training. Prior to allowing Personnel to access Customer Data, Service Provider and its subcontractors, agents, etc. (other than Pathway and AWS, which shall collectively be hereinafter referred to as "Excepted Subcontractors") will use commercially reasonable efforts to conduct background checks and ensure that all individuals have the reasonable skill and experience suitable for employment and placement in a position of trust and trained with respect to Service Provider's security policy and procedures. Service Provider shall not provide access to Customer Data if any such individual (other than Excepted Subcontractors'): (i) has been convicted of a felony or misdemeanor for fraud, theft, embezzlement, or other similar crimes involving dishonesty or breach of trust (or the equivalent thereof under relevant non-US law); (ii) is on any of the following lists: (a) the U.S. Government Specially Designated National and export denial list, (b) the OFAC List, (c) the BISDP List, (d) the OIG List, (e) the GSA List, or (f) any foreign equivalent; or (iii) for whom there is a significant deviation between the information reported by the individual and results of the background check.

(b) Architecture, Engineering, Application/Data Landscape Documentation. Service Provider must maintain current, accurate, and complete documentation on overall system, network, and application architecture, data flows and security functionality for applications that process or store Customer Data. Service Provider must employ documented secure programming guidelines, standards, and protocols in the development of applications or systems.

2.3. Technical Security Measures

(a) Security Event Logs. Security event-related logs must be preserved and be available online for a minimum of two (2) years. This requirement applies to the data sources that are capable of logging data that can be used to enforce accountability, detect a violation of security policy, detect an attempt to exploit vulnerabilities, and/or detect compromises resulting in losses of integrity, confidentiality and availability of Customer Data, environments, services, systems, and applications.

(b) Access and Authorization. Service Provider will employ physical, administrative, and technological access control mechanisms to prevent unauthorized access to Service Provider's facilities and systems associated with Customer Data, applications, and systems. Service Provider will limit access to Customer Data to Personnel with a need to know the information to perform the Services. Such mechanisms will have the capability of detecting, logging, and reporting access to the system or network or attempts to breach the security of the facility, compartment, system, network, application, and/or data.

(i) Each person must have an individual account that authenticates the individual's access to Customer Data. Service Provider will not allow sharing of accounts.

---

## PATHWAY TERMS AND CONDITIONS

---

(ii) Service Provider will utilize two-factor authentication .

(iii) Service Provider will maintain a process to review access controls quarterly for all Personnel who have access to Customer Data, applications, or systems, including any system that, via any form of communication interface, can connect to the system on which Customer Data is stored. Service Provider will maintain the same processes of review and validation for any third party hosted systems it uses that contain Customer Data.

(iv) Service Provider will promptly revoke a person's access to Customer Data within twenty-four (24) hours once such person no longer requires access to the system(s) or application(s) or immediately if warranted or requested by Customer.

(v) Service Provider will maintain a password policy that is consistent with recognized industry standards such as NIST Special Publication 800-63B.

(c) Data Transmission and Storage. Service Provider shall not transmit or store Customer Data outside the United States, Canada or Serbia, or allow its employees or agents to download, extract, store, or transmit Customer Data through personal computers, personal laptops, or other personal electronic devices , except where such devices may ordinarily be used by them in the performance of their duties or services for the Service Provider.

(d) Change Management. Service Provider will employ an effective documented change management program with respect to the Services. This includes logically or physically separate environments from production for all development and testing. No Customer Data will be transmitted, stored or processed in a non-production environment.

(e) Security Patch Management. Service Provider shall maintain and patch/remediate all systems, devices, firmware, operating systems, applications, and other software that process Customer Data consistent with Good Industry Practices.

(f) Network Security. Service Provider will deploy appropriate firewall, intrusion detection/prevention, and network security technology in the operation of the Service Provider's systems and facilities consistent with industry best practices. Traffic between Customer and Service Provider will be protected, authenticated, and encrypted.

(g) Malicious Code Protection. All workstations and servers must run anti-virus software, where possible and consistent with industry best practices.

(h) Data Encryption. Service Provider will utilize cryptographically secure protocols in accordance with Good Industry Practice at all times to encrypt Customer Data when in transit, at rest in any application or system, or transported/stored via any physical media (e.g. tapes, disks, etc.). If personal devices (e.g. desktops, laptops, mobile phones, tablets) are used to perform any part of the Services, Service Provider will encrypt all Customer Data on such devices and Service Provider will maintain an appropriate key management process, including, but not limited to, access controls to limit access to private keys, (both synchronous and asynchronous), key revocation processes, and key storage protocols (e.g., private keys must not be stored on the same media as the data they protect).

(i) Disaster Recovery. Service Provider warrants that it has and will maintain a Good Industry Practice disaster recovery plans in place that will allow Service Provider to resume full performance of the Services no

---

## PATHWAY TERMS AND CONDITIONS

---

more than twenty-four (24) hours after an interruption due to a disaster or other circumstance outside of Service Provider's control. If Service Provider fails to restore the Services within twenty-four (24) hours after an initial disruption, or if there are more than two interruptions of the Services during any twelve (12)-month period, Customer at its option may declare this Agreement immediately terminated for Cause by giving written notice to Service Provider, and Service Provider shall work with Customer in good faith to transition Customer to an alternative service provider as determined in Customer's sole discretion and at Service Provider's expense. Service Provider shall test such recovery plan at least once per year. Service Provider will discuss results of these tests with Customer on request. The Service Provider shall implement Good Industry Practice to securely back up data in respect of the Customer Data and promptly make such backed up data available to Customer on request.

3. Security Assessments. Service Provider's Security Program shall provide for regular assessment of the risks to the security of Customer Data and to Customer's, Service Provider's, or any third party's systems, applications, and services that are part of the Services. Service Provider shall promptly correct such deficiencies in accordance with the recommendations of such assessments, and, as applicable, this Schedule and the Agreement.

3.1. Security Risk Assessment. Customer acknowledges that Service Provider does not currently, but may in the future, perform SOC 1 SSAE 18 Type II .

3.2. Vulnerability Scans. Service Provider shall perform internal and external host/network vulnerability scans after any material change in the host/network configuration.

3.3. Application Security Tests & Assessments. Customer acknowledges that Service Provider will perform a security assessment, including a penetration test conducted by a reputable third party consistent with best practices in the information technology field, on applications and systems that process Customer Data within twelve months of the date of this Agreement.

4. Updates. Service Provider shall review and update its Security Program policies and procedures at least annually and as necessary to comply with changes in federal, state, and local laws and regulations pertaining to the privacy and protection of Customer Data. Service Provider shall ensure its Security Program stays current with industry best practices with respect to new security standards, threats and hazards. If Service Provider determines that it can no longer provide this level of protection, Service Provider will promptly notify Customer of this determination, and Customer shall have the right to terminate the Agreement upon notice to Service Provider without penalty or further liability. Upon request, Service Provider shall provide Customer a copy of the updated policies and procedures along with a report outlining material changes to Service Provider's systems, applications, and security program. Service Provider shall also provide a document containing key security management details (e.g. key contacts, incident response steps, back-up site information, details of processes to follow etc.) and notify Customer of any relevant updates.

5. Subcontractors. Service Provider shall conduct appropriate due diligence on any subcontractors (other than Excepted Subcontractors) involved in performing the Services or who have access to Customer Data, applications, or systems to ensure compliance not materially less protective than the standards included in this Agreement. Service Provider shall include and enforce obligations regarding data security in all its contracts with parties (other than Excepted Subcontractors) that have access to or process Customer Data, which obligations are no less protective than the standards included in this Schedule.

---

## PATHWAY TERMS AND CONDITIONS

---

6. Termination Due to Security Breach. Should Customer determine that Service Provider had a material security breach that resulted in unauthorized disclosure of Customer Data or that, in Customer's reasonable discretion, represents a material security risk, Customer shall have the right, in addition to all other rights and remedies under the Agreement or applicable law, to terminate the Agreement upon written notice to Service Provider.

7. Security Incident Response and Reporting. A security "Incident" is any event that could negatively impact the security of Customer Data and/or Customer's network (including any circumstances that would render such access or use reasonably possible and any breach of these Data Security Standards) including any (i) unauthorized, accidental or unlawful loss, access, use, disclosure, modification, or destruction of Customer Data; (ii) act that violates any law or any Customer or Service Provider security policy; (iii) unplanned service disruption that prevents the normal operation of the Services; or (iv) unauthorized access or attempt to access Service Provider's or Customer's applications, systems or Customer Data. If Service Provider detects or suspects an Incident, Service Provider shall:

7.1. Notify Customer's IT Security Representative by emailing the Client immediately and no later than within one (1) hour after Service Provider becomes aware of a security Incident involving regulated data (PHI, PCI, SOX, etc.) or Customer Data. For any other Incidents, notify Customer's IT Security within 24 hours. Customer shall retain the right to make and control any regulatory notifications required by an Incident.

7.2. Immediately perform such Incident response activities as may be reasonably requested by Customer, including, but not limited to: responding and investigating; collecting, analyzing and preserving evidence; and containing, remediating, recovering and mitigating adverse impacts. Service Provider will cooperate with Customer and with law enforcement authorities in investigating any such Incident, at Service Provider's expense. Service Provider will likewise cooperate with Customer and with law enforcement agencies to notify injured or potentially injured parties in compliance with applicable law, and offer identity theft monitoring services to injured or potentially injured parties at Customer's election; and such cooperation, including all costs associated with notifications and/or identity theft monitoring services as set forth above, will be at Service Provider's expense, except to the extent that the Incident was caused by Customer. The remedies and obligations set forth in this subsection are in addition to any others Customer may have.

7.3. If requested by Customer, prepare and deliver to Customer as soon as reasonably possible and no later than within five (5) business days of the Incident a root cause report that describes in detail (i) the nature and extent of the Incident; (ii) the Customer Data affected and the likely impact upon it; (iii) all supporting evidence, including system, network, and application logs related to the incident; (iv) all investigative, corrective and remedial actions completed, and planned actions and the dates that such actions will be completed; (v) all efforts taken to mitigate the risks of further Incidents; and (vi) an assessment of the security impact to Customer; and provide such further prompt assistance as Customer shall reasonably request in connection with notifications required to regulatory authorities under applicable law. Upon Customer's request, Service Provider shall provide Customer with immediate and ongoing access to all meetings, reports, copies of all logs and data, and other information that has a nexus to security Incidents impacting Customer.

8. Designated IT Security Representatives. Service Provider shall provide a designated contact person with responsibility for day-to-day security management to work with Customer's security organization. This individual shall be at an appropriate level and have the authority to initiate corrective actions on behalf of Service Provider

---

**PATHWAY TERMS AND CONDITIONS**

---

as necessary to respond to and correct any Incident, disclosure or breach involving Customer Data. If software development is involved, Service Provider shall also identify the person who will be responsible for overall security of the application development, management, and update process. The following individuals are Customer's and Service Provider's security representatives. All notifications required under this Schedule shall be made to such designated individuals.