24-7 INTOUCH CHANGE ORDER #009

The purpose of this Change Order is to clearly identify the need or request expressed in relation to the respective Statement of Work and provide a formal solution that will be implemented against such Statement of Work upon signature approval.

Client:	Government of Manitoba		
Project Name:	Vaccine Booking	**Program:**	GovMB Test Booking
Requestor:	Adam Topp	**Email:**	17(1) & 17(3)(e)
24-7 Intouch Sponsor:	17(1) & 17(3)(e)	**24-7 Intouch Email:**	17(1) & 17(3)(e)
Request Date:	December 9, 2020	**Effective Date:**	Dec 11, 2020
24-7 Intouch Change ID:	18(1)(b) & 20(	**Priority:**	High
MSA/SOW ID:	Government of Manitoba, and 24-7 Intouch Inc. ("Contractor") are parties to a Statement of Work dated APR 15, 2020 (the "SOW"), made pursuant to a Master Services Agreement dated APR 13, 2020 and amended on NOV 24, 2020 (the "MSA").		

CHANGE TO BE IMPLEMENTED

SUMMARY

24-7 Intouch Inc. ("Contractor") and Government of Manitoba ("Manitoba") agree to implement Vaccine Appointment Booking services as "Services", in which Contractor will take calls from residents of the Province of Manitoba and book Vaccine testing appointments on their behalf using a third party software booking tool (PetalMD) licensed by Manitoba.

Pursuant to the MSA and SOW referenced above, Contractor and Manitoba have mutually agreed to the following change(s).

SECTION II - SERVICE SOLUTION

Section II of the SOW will be amended as follows:

- The current Section 1 shall be renumbered to 1. a. and the following shall be added underneath it:
  b. As of December 12, 2020, the Contractor shall provide inbound call support to residents of the Province of Manitoba desiring to book vaccine appointments via an applicable phone number procured and provided by 24-7 Intouch, including taking applicable information from such persons and booking Vaccine appointments on their behalf through third party software licensed and made available by Manitoba, specifically, software provided by PetalMD (the "Additional Services").

    i) The Contractor shall configure a Greeting Front that callers shall listen to before being routed to an agent. Manitoba shall provide the script in both English and French to be read in the Greeting Front. Once a caller affirms they would like to continue with booking an appointment by pressing the appropriate button, the call shall be routed to the next available agent. The call routing mechanism shall prioritize these calls over all others routing to the same agent pool.

    ii) The Contractor shall configure an after-hours message that will be relayed to callers when the contact center is closed. Manitoba shall provide the script to be read for this after-hours message in both English and French.

    iii) The Contractor shall configure an "all appointments booked" message to be enabled once the available appointments have been exhausted. Manitoba shall provide the script to be read in both English and French. Manitoba, PetalMD, and 24-7 Intouch shall collaborate to measure the exhaustion of available appointments each day; Manitoba shall ultimately decide when this message shall be enabled. Once this message is enabled, this message will be relayed to all callers and no calls shall route to any agent until the original Greeting Front is re-enabled.

    iv) The Contractor shall leverage in-house talent to record the Manitoba-provided scripts. Manitoba may request adjusted messaging from time-to-time; the Contractor shall make commercially reasonable efforts to enable all requested changes within 24 hours of receipt. Time and effort expended by Professional Services to make the changes shall be billable.

The following shall be added under Section 3 b.:
c. Agents supporting the Additional Services will receive inbound calls from individuals seeking to book an appointment at a vaccination facility, and:

i. Agents shall navigate a Manitoba-provided eligibility questionnaire script with the caller to determine whether or not the caller is eligible to be booked for a vaccination. The Agent shall in no way be responsible for conferring any interpretation of symptoms or health status. The Manitoba-provided script shall allow for the Agent to direct the caller to the caller's health practitioner or online resources to clarify questions;
ii. Agents shall assist with locating the vaccination facility most convenient for the caller;
iii. Agents shall confirm available time slots; and

iv. Agents shall book callers into the system by gathering certain personal information (limited to First and Last Name, Phone Number, Email and MB Health Number).

The following shall be added under Section 4 c.:
d. The Hours of Operation for the provision of the Additional Services shall be 6am-8pm Central Time 7 days per week. At the launch of the program, the Parties agree that hours of operation may need to be adjusted with short notice; if Overtime is required in order to adjust, Manitoba shall approve such Overtime in writing (email is sufficient).

SECTION III - TECHNOLOGY SOLUTIONS

Section III of the SOW will be amended as follows:

The following table shall be appended to the existing table in Subsection 3a of Section III of the SOW:

TECHNOLOGY	NAME OF SYSTEM	RESPONSIBILITY
Appointment Booking Tool	PetalMD	Manitoba
Eligibility Screening Tool	Digital Health	Manitoba
Greeting Front	Five9	24-7 Intouch
Telephony	Five9	24-7 Intouch

The following shall be added below the table in Subsection 3 of Section III of the SOW:

b. For the purposes of fulfilling Contractor's obligations with respect to the Additional Services, Contractor agents shall be required to ask individual callers for certain personal health information ("PHI"), limited to First and Last Name, Phone Number, Email and MB Health Number. The agents shall input these details directly into the PetalMD booking system which has been licensed and made available by Manitoba and shall keep no other record on these details. Manitoba may request Contractor agents to ask certain other questions of individual callers including occupation, and whether the caller self-identifies as First Nations, Inuit, or Metis. This information, and the responses to Manitoba's eligibility screening tool, shall be captured in Manitoba's provided Digital Health tool.

c) The Parties agree that the act of inputting the aforementioned PHI into the PetalMD booking system and Digital Health eligibility screening tool as part of the Additional Services is an approved action and does not constitute a breach of the Agreement, including the provisions regarding the protection of Confidential Material therein and the provisions regarding the protection of personal information included in Exhibit 1 to Schedule B of the Remainder of the Agreement.

d) For greater certainty, the Parties agree that the access, use, disclosure, security, and maintenance of all data inputted to and stored in PetalMD or Digital Health is subject to the unique contractual agreement between Manitoba and PetalMD or Digital Health. Contractor shall have no liability whatsoever in relation to the PetalMD booking system or Digital Health, including with respect to any access to, use of, or data inputted by Contractor or its agents into, the PetalMD booking system or Digital Health and, accordingly and notwithstanding anything in the Agreement to the contrary (including Section 6.4 of Schedule B of the Remainder of the Agreement), Manitoba agrees to fully indemnify Contractor for any and all damages, losses, liabilities, expenses and costs suffered or incurred by Contractor in connection with any of the foregoing.

The following shall be added to Subsection 4 of Section III of the SOW:

e. The parties agree that the reporting for the Additional Services will include emailed interval and end of day statistical

reports. The interval and end of day reports shall be subject to change from time to time, but are intended to showcase the following:

- Overall volumes
- Longest wait times
- Overall program management notes (i.e. how things are going)
- Any issues/concerns

SECTION IV - STAFFING SOLUTIONS

Section IV of the SOW will be amended as follows:

The following shall be added to Subsection 1 of Section IV of the SOW:

i. In accordance with its protection of personal information obligations under Exhibit 1 to Schedule B of the Remainder of the Agreement, Contractor agrees that Contractor shall require all agents, operations leadership, and support resources assigned to the Additional Services to review their privacy obligations and sign off on a Contractor Pledge of Confidentiality Agreement prior to working on the Additional Services

PRICING

Agent hours for the Additional Services shall be invoiced in the same manner/price as the other Services (as per the SOW).

The following one time change-related costs are specific to launching the Additional Services:

Description	Units	Fees (CAD):
Implementation Fee ● Covers the installation of the Project described herein. Includes procurement of Vanity TFN (1), project management, support services, and administration related to launch.	One Time	18(1)(b) & 28(1)(b)
IT Development - TFN Configuration and IVR deployment (2 lines) ● Add rush fees 18(1)(b) & 28(1)(b)	4 Hours	
IT Development - Reporting Changes ● Add rush fees 18(1)(b) & 28(1)(b)	2 Hours	
IT Development - Systems Configuration and Testing ● Add rush fees 18(1)(b) & 28(1)(b)	3 Hours	
Training Curriculum Design/Development ● Add rush fees 18(1)(b) & 28(1)(b)	2 Hours	
	SUBTOTAL:	
Agent Up-Training	1 hr / agent	

APPROVAL

The parties agree that this Change Order shall be made to the SOW, effective as of the date set out above. Except as specifically modified by this Change Order, all terms and conditions of the SOW remain unchanged and in full force and effect. This Change Order shall be appended to the SOW once fully executed.

GOVERNMENT OF MANITOBA		24-7 INTOUCH INC.	
Signature	17(1) & 17(3)(e)	**Signature:**	DocuSigned by: 17(1) & 17(3)(e)
Name:	Paul Beauregard	**Name:**	
Title:	Secretary to Treasury Board	**Title:**	President
Date:	December 11, 2020	**Date:**	Dec-12-2020

24-7 INTOUCH AUTHORIZATION FORM

The purpose of this Authorization is to clearly identify the need or request expressed and approval to proceed with the solution as documented.

Client:	Government of Manitoba		
Project Name:	Five 9 - Callback Functionality	**Program:**	Gov't of MB Vaccine
Requestor:	Adam Topp	**Email:**	17(1) & 17(3)(e)
24-7 Intouch Sponsor:	17(1) & 17(3)(e)	**24-7 Intouch Email:**	17(1) & 17(3)(e)
Request Date:	January 8, 2021	**Effective Date:**	January 8, 2021
Ref#:	10247	**Priority:**	High

AUTHORIZATION TO BE IMPLEMENTED

SUMMARY

- In order to configure and release Five9's callback functionality for use on Gov of MB's Vaccine Booking program, 24-7 Intouch shall incur Professional Services workload that is billable.
- 24-7 Intouch will also develop training and deliver training to agents to ensure a smooth rollout of the product. Training development and training time will both be billable.
- The Parties acknowledge that the caller's phone number shall be temporarily stored in Five9 in order to issue the call back. Such storage shall occur on Five9's US-based data center.

PRICING

Description	Units	Fees (CAD):
Telecom - training, setup, and configure	18(1)(b) & 28(1)(b)	
Training Development @		
Agent Training @ 30 minutes per agent		
	TOTAL:	

APPROVAL

Signature Record of Approval

GOVERNMENT OF MANITOBA	
17(1) & 17(3)(e)	
Name:	Paul Beauregard
Title:	Secretary to Treasury Board
Date:	January 14, 2021

24-7 INTOUCH INC.	
Signature:	
Name:	17(1) & 17(3)(e)
Title:	
Date:	

26 [redacted]

This Agreement is between the Government of Manitoba ("**Manitoba**") 2nd Floor-270 Osborne Street North Winnipeg, MB R3C 1V7, email: Gary.Luedtke@gov.mb.ca, and 24-7 Intouch Inc. ("**Contractor**") 17(1) & 17(3)(e) [redacted] 17(1) & 17(3)(e) for the purchase of certain services dated April 13, 2020 ("**Effective Date**").

1. **Term**: This Agreement starts on April 13, 2020 and will continue for a period of six (6) months, ending October 12, 2020, unless terminated earlier in accordance with the terms hereof or extended by Manitoba for up to two (2) extensions of three (3) months each on the same terms as in this Agreement, in each case, by Manitoba providing at least sixty (60) days' prior written notice to the Contractor of its intention to do so (the "**Term**").

2. **Documents**: This Agreement is comprised of this first page and the following schedules:
   (a) Schedule A – Services
   (b) Schedule B - Terms and Conditions
   (c) Schedule C – Statement of Work (will be incorporated by reference once completed in accordance herewith)

   In the event of conflict, the order of priority is this first page, Schedule B (Terms and Conditions), Schedule C (the Statement of Work) and Schedule A (Services).

3. **Terms and Conditions**: The terms and conditions in Schedule B apply to the purchase of the Services (as defined in Schedule B).

4. **Services**: The Contractor will provide the Services in accordance with the terms and conditions in this Agreement. Manitoba has no liability with respect to any Services provided by the Contractor prior to the start of the Term or provided following the Term.

5. **No Exclusivity**: This Agreement does not confer exclusivity on the Contractor, or limit or prohibit Manitoba from performing itself, or using any third party other than the Contractor to provide the Services.

6. **No Volume Commitment:** Manitoba makes no commitment or representation as to the number of in-bound or outbound calls that will be required or that will occur during the Term.

7. **Fees**: All invoices in respect of the Services provided hereunder shall be submitted electronically to Gary.Luedtke@gov.mb.ca, with all supporting documentation reasonably requested by Manitoba, and all fees in respect thereof will be paid in accordance with Section 4 in Schedule B.

8. This Agreement may be executed in counterparts, each of which will be deemed to be an original of this Agreement and together will constitute one and the same instrument. Delivery of this Agreement (including an executed signature page) by any party by electronic transmission will be as effective as delivery of a manually executed copy of this Agreement by such party.

THIS AGREEMENT has been executed on behalf of the Government of Manitoba and the Contractor, by their duly authorized representatives, on the dates noted below.

THE GOVERNMENT OF MANITOBA

17(1) & 17(3)(e) [redacted]

Minister of Finance (or designate)
Name: Paul Beauregard
Date: April 13, 2020

24-7 INTOUCH INC.

17(1) & 17(3)(e) [redacted]

Date: Apr-13-2020

SCHEDULE A – SERVICES

The Contractor will provide the Services and Deliverables in accordance with the terms hereof (including, for greater certainty, the Statement of Work to be entered into by the parties no later than April 15, 2020 (the "Statement of Work"). Once completed the Statement of Work will be incorporated by reference and form an integral part of this Agreement.

1. The Contractor shall commence the following services (the "Set Up Services") on April 13, 2020 and, unless otherwise provided for in this Agreement, complete such services in accordance with the timelines specified in the Statement of Work:

    (a) develop an implementation project plan that adheres to Manitoba's timelines to meet the agreed upon initial operational launch date of Thursday, April 16, 2020
    (b) train for outbound calls;
    (c) work with Manitoba project management to outline all steps, roles and responsibilities of both parties to ensure smooth and timely implementation of service initiatives; and
    (d) deliver the following implementation cadence as part of the transition:
        Assignment of Project Manager (PM) and action team, to include recruiting, training, operations, IT, WFM and professional services members from the Contractor; and
        (i) provide Manitoba with project status on key milestones throughout the initial implementation of services and resolve any issues that may delay implementation.

2. Subject to the Statement of Work, the Services shall include:

    (a) Call centre services, including out-bound and in-bound call activities, to help inform and guide affected Stakeholders (as defined in Schedule B) in COVID-19 pandemic to access government supports, resources and opportunities that will help allow their businesses to remain viable in the long-term.

        (i) Out-bound Call Activities

            (A) Purpose: To proactively reach out to the Stakeholders to provide information on supports, resources and opportunities available to assist in challenges related to COVID-19.

            (B) The out-bound call activities shall commence on April 16, 2020 and the Contractor shall attempt to reach out to an estimated 65,000 Stakeholders no later than April 27, 2020.

        (ii) In-bound Call Activities

            (A) Purpose: To support the Stakeholders in accessing supports, resources and opportunities available.

            (B) Certain in-bound call activities shall commence on April 17, 2020.

            (C) Scripts for call takers are to be developed by the Contractor leveraging professionals engaged by the Contractor that have finance and accounting expertise. The Contractor shall develop such scripts by following conceptual direction provided by Manitoba. Scripts and must be acceptable to Manitoba.

3. Subject to the Statement of Work, staffing in respect of the Services will be as follows:

   (a) Location:

      (i) All call takers must be located in Canada.

      (ii) The primary call centre will be located in the Province of Manitoba, provided that any call taker may provide the Services from his or her home in Canada provided that the Contractor (including the call takers) continues to comply with all its obligations under this Agreement including confidentiality and security.

      (iii) No calls shall be routed outside of Canada, and none of the data used by the call centres shall be stored outside of Canada.

   (b) Training:

      (i) Call takers must receive training in order to provide timely and accurate information to callers.

      (ii) Support may be required from finance and accounting professionals, including tax professionals, to ensure that scripts (developed following conceptual guidance provided by Manitoba) for staff are timely and accurate.

4. At the Stakeholder's request, a Stakeholder shall have the ability to choose to speak with an alternate representative or supervisor in the Province of Manitoba. In the event a call-taker recognizes that the call taker has been asked to call or has called a Stakeholder who is known to the call taker, the Contractor shall cause the call taker to transfer the Stakeholder to an alternate representative or supervisor.

5. Services must be provided in English and French. The Services must be operational from during the hours specified in the Statement of Work seven (7) days a week.

6. Subject to the Statement of Work, IT system requirements in respect of the Services will be as follows:

   (a) The Contractor will, in real time, track call centre activities, including the extent to which applicable service metrics to be set out in the Statement of Work are met.

   (b) The Contractor will produce and provide to Manitoba daily reports that summarize the call centre activities in respect of the Services. These reports must include applicable service metrics set out in the Statement of Work identifying achievement separately for both English and French support.

   (c) The Contractor will track Stakeholder support requests if multiple interactions are required.

7. The Contractor shall cooperate with any reasonable request by Manitoba or any of its Representatives related to any Manitoba endorsed media advertising campaign related to the Services with the goal to drive Stakeholders to the call centre services, provided that the Contractor shall not be required to make any public comment or disclosure with respect to this Agreement. Such cooperation shall include providing Manitoba any data or other information obtained by the Contractor in connection with the Services (including, for example, success stories of Stakeholders who were able to access federal support as a result of the Services).

SCHEDULE B – TERMS AND CONDITIONS

1. DEFINITIONS

1.1 **"Business Day"** means Monday through Friday, excluding statutory holidays in the Province of Manitoba, between the hours of 8:00 a.m. and 6:00 p.m. (Winnipeg Time).

1.2 **"Confidential Material"** means all information, data, documents and materials acquired by one party, or to which access has been given to one party in the course of, or incidental to, this Agreement and includes Personal Information but excludes information, data, documents and materials if they:

(a) were in the public domain or known to the receiving party prior to the time of disclosure, or become publicly available other than through a breach of this Agreement; or

(b) become known to the receiving party from a source other than the disclosing party without breach of any duty of confidentiality; or

(c) are approved, in writing, for disclosure without restriction by the disclosing party; or

(d) are developed independently by the receiving party without reference to the Confidential Material of the disclosing party and without a breach of any duty of confidentiality.

1.3 **"Deliverables"** means information, documents and materials produced by the Contractor, or any of its Representatives, in the performance of the Services under this Agreement, including the Project Plan, Service Implementation Plan and Risk Assessment and Mitigation Plan (in each case, as attached to the Statement of Work) and any training materials and call scripts related to the Services.

1.4 **"Key Personnel"** means Contractor's key personnel and employees, and key personnel and employees of the Contractor's approved subcontractors, identified in the Statement of Work, or as otherwise mutually agreed to by the parties.

1.5 **"Manitoba Data"** means any data, information or material:

(a) made available by Manitoba to the Contractor for the purposes of this Agreement;

(b) respecting Stakeholders obtained, accessed or received by the Contractor from whatever source in connection with the performance of the Services; and

(c) with respect to data only, generated by the Contractor as part of the Services.

1.6 **"Personal Information"** has the meaning given to that term in Exhibit 1 to Schedule B.

1.7 **"Representatives"** means the directors, officers, officeholders, employees, consultants, business partners, agents and subcontractors of a party and any other party for whom that party is responsible at law. In the case of the Contractor, "Representatives" includes Key Personnel.

1.8 **"Services"** means the services set out in Schedule A (including the Set Up Services) and any other services described in the Statement of Work to be delivered by the Contractor in accordance with this Agreement.

1.9 **"Stakeholders"** means any:

(a) business which employs individuals in the Province of Manitoba (including self-employed individuals and sole proprietorships operating in the Province of Manitoba); and

(b) charities and/or not-for-profit organizations employing or engaging individuals;

which are otherwise operating within the Province of Manitoba.

2. INTERPRETATION

2.1 Unless otherwise specified in this Agreement:

(a) all documents and materials, including invoices and reports, to be provided by the Contractor must be satisfactory in form and content to Manitoba, acting reasonably;

(b) any and all agreements, approvals or consents of a party required hereunder must be in writing;

(c) words denoting inclusiveness (such as "including" or "includes") shall not be deemed to be exhaustive;

(d) discretions, options, elections or other similar words used with respect to a party, are deemed to mean such party's sole and absolute discretion, option, election or other such similar act;

(e) references to currency in this Agreement and all invoices and payments will be in Canadian dollars; and

(f) references to statutes include all regulations made under that statute as existing or replaced from time to time.

2.2 No provision of this Agreement shall be interpreted against any party merely because that party or its legal representative drafted the provision.

3. REPRESENTATIONS AND WARRANTIES AND PERFORMANCE OF CONTRACTOR'S OBLIGATIONS

3.1 The Contractor represents and warrants that the Contractor possesses the necessary personnel, skills, expertise and experience to provide the Services in accordance with the provisions of this Agreement. The Contractor acknowledges that Manitoba has entered into this Agreement relying on these representations and warranties.

3.2 The Contractor agrees:

(a) Subject to Section 3.3, that the Key Personnel shall be dedicated to the provision of the Services and not replaced or re-assigned during the Term, unless Manitoba agrees otherwise in writing provided that nothing herein shall limit the removal of any Key Personnel in the event that such Key Personnel is no longer employed by the Contractor (or its applicable subcontractor) or their respective affiliates;

(b) that the Contractor and its applicable Representatives shall devote the time, attention, abilities and expertise necessary to perform the Contractor's obligations under this Agreement;

(c) the Contractor's staff taking calls in connection with the provision of the Services will be duly trained in order to provide timely and accurate information to Stakeholder callers;

(d) the Contractor will enlist the support of finance and accounting professionals, including third party tax professionals, to ensure that scripts for staff taking calls in connection with the provision of the Services are timely and accurate;

(e) all obligations hereunder will be performed, and the Services will be provided in, a professional manner; and

(f) to comply with all applicable laws and regulatory requirements, whether federal, provincial or municipal, in connection with the provision of the Services.

3.3 If Manitoba determines, in its discretion, acting reasonably, that any individual providing Services poses a security or other material risk to Manitoba, the Contractor will within twenty-four (24) hours of receiving notice from Manitoba with respect thereto, remove such individual from the provision of the Services. Any request by Manitoba for removal of personnel will not be considered to be a request for a termination of employment, engagement or other relationship between the individual and the Contractor. Any decision to terminate an employment, engagement or other relationship with the individual will be made solely by the Contractor.

3.4 Manitoba represents and warrants that: (i) the Contractor is permitted to use the contact information to be provided by Manitoba to the Contractor in relation to the provision of the Services for the purpose of providing the Services, and (ii) such information will have been provided to the Contractor for its use in the provision of the Services hereunder, in accordance with all applicable laws.

4. FEES

4.1 Manitoba shall pay to the Contractor the fees specified in the Statement of Work.

4.2 In the event that the parties are unable to agree to a Statement of Work on or before April 15, 2020 (or such other date mutually agreed to by the parties), Manitoba shall pay to the Contractor:

(a) the fees incurred for the Set Up Services performed, and

(b) any out of pocket costs reasonably and actually incurred (i.e., no mark-up) in connection with the Set Up Services,

in each case, during the period between April 13, 2020 and April 15, 2020 (inclusive) and in accordance with the rates and costs set out in Exhibit 2, up to a maximum amount of [redacted] 18(1)(b) & 28(1)(b) (the "Set Up Fee"). The Contractor shall provide Manitoba any information or documentation reasonably requested in order to substantiate the Set Up Fee. The Set Up Fee shall be the Contractor's sole and exclusive remedy for the parties failing to agree to a Statement of Work.

4.3 Manitoba shall pay all undisputed invoices within sixty (60) days of Manitoba's receipt of the applicable invoice. For greater certainty, Manitoba shall not dispute any invoice in bad faith. Undisputed invoices that have not been paid by Manitoba within such sixty (60) day period shall bear interest in accordance with the provisions of the Government of Manitoba's Financial Administration Manual issued under the authority of *The Financial Administration Act* from the 61st day after the date of invoice until payment is made. Relevant excerpts of the Financial Administration Manual will be provided to the Contractor on request. For greater certainty, once any disputed invoice is resolved between the parties, Manitoba shall, upon receipt of an invoice in respect of the applicable resolved amount, pay to the Contractor the applicable resolved amount in accordance with the terms of this Section 4.3.

4.4 Manitoba certifies that the Services being provided pursuant to this Agreement are being purchased with Crown funds for the benefit of the Government of Manitoba and are therefore not subject to the payment of the federal goods and services tax ("GST"). Manitoba's GST number is R107863847. The Contractor must not include GST in any invoice provided or claim for payment made under this Agreement

4.5 Notwithstanding any other provision of this Agreement, the payment of fees by Manitoba is conditional upon there being an appropriation of funds available from the Legislature of the Province of Manitoba for payments by Manitoba in the fiscal year in which they are required to be paid by Manitoba (for the purpose of this clause, fiscal year means April 1 of one year to March 31 of the next year).

4.6 If Manitoba is obligated by law or international treaties or conventions to withhold or deduct taxes from any payment of fees to the Contractor, Manitoba shall remit such withheld amounts as required by the *Income Tax Act* (Canada) or under the terms of any other law or international treaty or convention to which Manitoba is subject, and shall furnish to the Contractor official receipts evidencing Manitoba's payment of such taxes. The Contractor will be solely responsible for obtaining a refund with respect to any amounts withheld pursuant to this Section 4.5.

5. CONFIDENTIALITY, SECURITY AND PERSONAL INFORMATION

Confidentiality

5.1 While this Agreement is in effect and at all times thereafter, the Contractor and Manitoba and their respective Representatives who receive Confidential Material from the other party shall treat that Confidential Material as confidential, with the same degree of care as the receiving party uses to protect its own Confidential Material, but no less than with a reasonable degree of care.

5.2 The receiving party shall:

(a) not use or reproduce Confidential Material of the disclosing party for any purpose other than as and to the extent expressly permitted under this Agreement or as may be reasonably necessary for the exercise of its rights or the performance of its obligations under this Agreement;

(b) not disclose, provide access to, transfer or otherwise make available any Confidential Material of the disclosing party, except as expressly permitted in this Agreement; and

(c) promptly notify the disclosing party in writing of any unauthorized access, use, dissemination or publication of Confidential Material of which it becomes aware.

5.3 The receiving party may disclose the disclosing party's Confidential Material:

(a) to the receiving party’s Representatives but only if and to the extent that such persons need to know the Confidential Material to perform their obligations under this Agreement, and

(b) to the receiving party’s accountants, internal and external auditors, legal counsel and other professional advisors but only if, and to the extent that such persons need to know the Confidential Material to provide applicable professional advisory services relating to the receiving party’s business or affairs,

on condition that such persons are made aware before such disclosure of the confidential nature of the Confidential Material and are subject to terms of confidentiality that are at least as stringent as the terms of this Section 5 or, in the case of persons described in clause 5.3(b), a duty of confidence exists between the receiving party and such person;

(c) upon prior written notice to the disclosing party, as required by law or regulation to be disclosed or as required by order of a court or other governmental body, but only to the extent and solely for the purpose of such required disclosure; and

(d) in Manitoba's case, as required to enable Manitoba to satisfy its obligations under the terms of any trade agreements, international treaties or conventions to which it is subject.

The receiving party will assist the disclosing party (at the disclosing party's expense) in all proper ways to limit or prevent the disclosure of such Confidential Material.

5.4 Disclosure of any Confidential Material pursuant to subsection 5.3 will not be deemed to render it non-confidential and the receiving party's obligations with respect to such Confidential Material shall not be changed or lessened by virtue of any such disclosure.

5.5 Subject to subsection 5.6, upon the earlier of termination of this Agreement and the disclosing party's request, the receiving party will promptly return or destroy (at the disclosing party's election) all Confidential Material and, where the Contractor is the receiving party, all Manitoba Data, acquired by the receiving party or any of its Representatives. Notwithstanding the foregoing, the Contractor shall be permitted to retain such copies of Confidential Material to the extent: (i) required by law; or (ii) such copies are embedded in the automated backup of electronic data processing systems, provided that the Contractor shall (i) continue to be bound by obligations of confidentiality with respect to such Confidential Material as set out herein; and (ii) with respect to copies embedded in the Contractor's backup systems, delete any such Confidential Material in accordance with the Contractor's deletion policies, which shall be purged no less than every ninety (90) days. For clarity, this obligation shall apply to any subcontractor which possess Manitoba Data in connection with the Services.

5.6 Confidential Material provided by the Contractor to Manitoba that is legislatively classified or defined as "government records" will be returned or destroyed by Manitoba in accordance with the applicable legislation.

5.7 Other than as required by law or any governmental authority, the Contractor will not make or issue any public communications or respond to media inquiries related to the Services or this Agreement without Manitoba's prior written approval.

5.8 Manitoba will not make or issue any public communications or other public disclosure regarding any of the terms of this Agreement or identifying the Contractor by name except to the extent (i) required by law (including applicable trade agreements) or Manitoba's internal policies; or (ii) consistent with Manitoba's practices. Manitoba acknowledges the importance of protecting the Contractor's Confidential Material. To the extent Manitoba receives a request to disclose any Contractor Confidential Material pursuant to applicable law, without limiting any rights of the Contractor or obligations of Manitoba under applicable law, Manitoba agrees to make all reasonable efforts to give the Contractor the opportunity to provide input as to what Confidential Material should be redacted as permitted by applicable law.

SECURITY

5.9 While using Manitoba's facilities pursuant hereto, the Contractor and its Representatives must comply with all reasonable security requirements of Manitoba communicated by Manitoba to the Contractor in writing.

5.10 The Contractor will comply with and undertake the security measures, practices and procedures described in the Statement of Work.

5.11 Without limiting the obligations in subsection 5.9:

(a) Each year during the Term, the Contractor will engage an independent third party to conduct a security audit of the Contractor, and the Contractor will provide copies of all such audit reports to Manitoba upon request.

(b) The Contractor will have in place business continuity and disaster recovery plans and procedures applicable to the Services and the Contractor's sites where the Services are carried out of (including the datacentres), which includes all subcontractors involved in delivery of the Services. The Contractor will provide copies of those plans and procedures to Manitoba on request.

(c) The Contractor will, no less frequently than annually, review and test its business continuity and disaster recovery plan.

(d) Upon request, the Contractor will provide Manitoba with monthly reports respecting its vulnerability and security testing of the Services.

5.12 Data Centre

(a) The Contractor represents that as of the Effective Date, it has a datacentre in Winnipeg, Manitoba.

(b) Notwithstanding anything to the contrary in this Agreement, the primary datacenter in respect of the Services must be located in the Province of Manitoba.

5.13 The Contractor shall ensure that no subcontractor (including Salesforce) accesses Manitoba Data unless otherwise agreed to by Manitoba in writing.

5.14 The Contractor shall perform the criminal records checks (and associated diligence) in accordance with the Statement of Work.

Privacy

5.15 Where the Contractor will have access to any Personal Information, it shall comply with requirements respecting the collection, use, disclosure and destruction of Personal Information as set out in *The Freedom of Information and Protection of Privacy Act* (Manitoba) including the requirements set out in Exhibit 1 to this Schedule.

6. LIABILITY AND INDEMNIFICATION

6.1 Except to the extent caused or contributed to by Manitoba, the Contractor shall indemnify and hold harmless and defend Manitoba in respect of third party claims made against Manitoba for any injury to persons (including death), damage or loss to property or infringement of rights caused by the negligence or willful acts or omissions of the Contractor or its Representatives in connection with the Agreement or breach of this Agreement by the Contractor or its Representatives. Notwithstanding anything in this Agreement to the contrary, the third party claims in this subsection 6.1 are not subject to any exclusions or financial limits, whether or not classified as resulting in indirect damages (including without limitation Section 6.4).

6.2 With respect to any third party claim arising under subsection 6.1:

(a) Manitoba will promptly inform the Contractor, in writing, of any such claim or demand and allow the Contractor, at the Contractor's cost, to control the defence and any related settlement negotiations. The Contractor may proceed to settle any claim without Manitoba's consent if such settlement does not require any out of pocket payments by Manitoba and does not require admission of liability by Manitoba.

(b) A failure to promptly notify the Contractor of any claim will only affect the Contractor's obligations under subsection 6.1 to the extent that Manitoba's failure materially prejudices the Contractor's ability to defend the claim or demand.

6.3 The Contractor's total cumulative liability for all direct claims, damages, losses or costs sustained or suffered by Manitoba shall be limited to the greater of 18(1)(b) 18(1)(b) or the fees payable under this Agreement.

6.4 Neither party shall have any liability at any time for any indirect, special, or consequential damages, even if advised of the possibility of such damages.

6.5 The limitations set out in subsections 6.3 and 6.4 shall not apply to any liability or claim arising under subsection 6.1 or resulting from any criminal, fraudulent act or omission, or willful misconduct on the part of the Contractor or its Representatives.

6.6 Manitoba shall indemnify and hold harmless and defend the Contractor in respect of third party claims made against the Contractor as a result of Manitoba's breach of its representation and warranty in Section 3.4. Notwithstanding anything in this Agreement to the contrary, the indemnification obligations in this Section 6.6 are not subject to any exclusions or financial limits, whether or not classified as resulting in indirect damages (including without limitation Section 6.4).

7. INSURANCE

7.1 The Contractor will obtain and maintain, at its cost, throughout the Term:

(a) commercial general liability insurance against claims for personal injury and death and damage to property in the amount of 18(1)(b) per occurrence which shall name Manitoba (for greater certainty, the "Government of Manitoba"), its Ministers, its officers, employees and agents as Additional Insureds; and

(b) if providing professional services, errors and omissions insurance for negligent acts, errors or omissions of the Contractor and its Representatives, in the amount of 18(1)(b) 18(1)(b) per occurrence or claim, which shall be purchased and maintained during the Term and for a minimum of twelve (12) months after the end of this Agreement (or alternatively, the Contractor will purchase and maintain extended claims reporting coverage for that twelve (12) month period).

7.2 The Contractor will provide no less than thirty (30) days' prior written notice to Manitoba in the event of cancellation.

7.3 Each required insurance policy shall be underwritten by insurers licensed in Canada and be reputable and financially creditworthy insurers with an A.M. Best financial strength rating of "A-" or higher, or equivalent rating by an alternate insurance credit rating agency.

7.4 The Contractor shall ensure that all employees or subcontractors providing the Services are covered by workers' compensation insurance where such coverage is required by law.

7.5 The Contractor shall provide Manitoba with a Certificate of Insurance evidencing the insurance required in this Section. Thereafter during the Term, the Contractor will provide Manitoba with certificates of renewals upon request.

8. FORCE MAJEURE

8.1 In this Section:

(a) **"Affected Party"** means a party prevented from performing its obligations in accordance with this Agreement by a Force Majeure Event;

(b) **"Force Majeure Event"** means any unforeseen event that is beyond the reasonable control of a party that prevents such party from performing its obligations under this Agreement and may include the following:

(i) a natural disaster, fire, flood, storm, disease epidemic/pandemic or power failure;

(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy;

(iii) a freight embargo; or

(iv) any action by a governmental authority,

except that a Force Majeure Event will not include changes in market conditions or the financial hardship of a party.

8.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from a Force Majeure Event and any time periods for the performance of such obligations are automatically extended for the duration of the Force Majeure Event provided that the Affected Party complies with the requirements of subsection 8.3.

8.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Force Majeure Event and make all reasonable efforts to prevent, control or limit the effect of the Force Majeure Event, including activating its business continuity plans (as applicable), so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

8.4 If the Contractor is the Affected Party, it will continue to regularly provide communication to Manitoba as is reasonably practicable during the continuance of the Force Majeure Event.

8.5 Notwithstanding anything to the contrary in this Section, in the event the Contractor's performance under this Agreement is delayed for a period of five (5) consecutive Business Days or more as a result of a Force Majeure Event, Manitoba may terminate this Agreement immediately upon notice to the Contractor. Manitoba will consult with the Contractor to discuss the Contractor's circumstances, concerns and potential work-arounds before exercising this right of termination.

8.6 Notwithstanding anything to the contrary, the parties agree that a Force Majeure Event shall not relieve either party of its confidentiality obligations under this Agreement.

9. TERMINATION

9.1 Manitoba may at any time terminate this Agreement for convenience on five (5) days' notice in writing to the Contractor provided that, in the event Manitoba provides less than sixty (60) days prior written notice, Manitoba shall pay to the Contractor any out of pocket costs reasonably and actually incurred (i.e., no mark-up) by the Contractor to wind down the Services as a result of such early termination, such costs not to exceed 18(1)(b) 18(1)(b) (the "Termination For Convenience Fee").The Contractor shall use reasonable efforts to mitigate all costs incurred by the Contractor as a result of such termination including reassigning personnel and negotiating agreements with subcontractors related to the provision of the Services on terms that will enable the Contractor to terminate such agreements upon conditions and terms which will minimize their cancellation and wind-down costs in the event of a termination of this Agreement. The Contractor shall provide Manitoba any information or documentation reasonably requested in order to substantiate the Termination For Convenience Fee. The Termination For Convenience Fee shall be the Contractor's sole and exclusive remedy for Manitoba terminating pursuant to this Section 9.1.

9.2 Without restricting any other remedies available:

(a) this Agreement shall automatically terminate in the event the parties are unable to mutually agree on a Statement of Work on or before April 15, 2020 or such other date mutually agreed to by the parties in writing;

(b) either party may immediately terminate this Agreement with written notice if the other party has failed to comply with any material term or condition of this Agreement, and has failed to remedy the failure within ten (10) Business Days following the receipt of the written notice of default; and

(c) Manitoba may immediately terminate this Agreement for cause with written notice if:

(i) Set Up Services do not commence on April 13, 2020;

(ii) The outbound call Services do not commence on or before April 16, 2020;

(iii) Services in their entirety do not commence in accordance with the Statement of Work; or

(iv) At any time following April 16, 2020, the Contractor fails to provide a minimum of 75% of the agreed upon staffing level outlined in the Statement of Work for

(a) any three (3) days over a fourteen (14) day period; or

(b) any five (5) days over a thirty (30) day period; or

(v) the Contractor is dissolved or becomes bankrupt or insolvent.

9.3 Upon the Contractor's receipt of the notice of termination:

(a) At no cost to Manitoba:

(i) the Contractor will promptly, but in any event within 24 hours, provide an export of all Manitoba Data in a standard, generally accepted industry standard electronic form, without any restriction on its use by Manitoba; and

(ii) within thirty (30) days thereafter, the Contractor will delete all copies of Manitoba Data from its servers. Back-ups of Manitoba Data will expire after deletion in accordance with the Contractor's routine procedures but no later than 90 days. For clarity, this obligation shall apply to any subcontractor which possess Manitoba Data in connection with the Services..

(b) The Contractor must cease to perform any further work and will only undertake such wind down activities as are authorized by Manitoba in writing. Manitoba will be under no obligation to the Contractor other than to pay, upon receipt of an invoice and supporting documentation, such compensation as the Contractor may be entitled to receive under this Agreement for work completed in satisfaction of this Agreement up to the date of termination.

10. OWNERSHIP OF MANITOBA DATA, DELIVERABLES AND EQUIPMENT

10.1 Manitoba reserves all title and ownership of the Manitoba Data. The Contractor shall make all Manitoba Data available at all times to Manitoba and all third parties authorized by Manitoba. Under no circumstances, including material or fundamental breach of this Agreement, will the Contractor withhold any Manitoba Data but shall return, release and/or provide access to all Manitoba Data immediately upon request by Manitoba.

10.2 Manitoba hereby grants the Contractor the right to use the Manitoba Data for the sole purpose of providing the Services.

10.3 Subject to subsection 10.4:

(a) all Deliverables and Manitoba Data generated as part of the Services (collectively, "**Work Product**") and all intellectual property rights in the Work Product (including all copyright, patent, trade mark rights) are and will be the exclusive property of Manitoba, and will be promptly delivered without cost to Manitoba upon request or when the Agreement is terminated or expires; and

(b) the Contractor hereby assigns and transfers, agrees to assign and transfer, and agrees to cause any subcontractors to assign and transfer, all right, title and interest (including all intellectual property rights) in and to all Work Product, as and when created, to Manitoba.

10.4 The Contractor retains all intellectual property rights in its methodologies, processes, techniques, ideas and concepts existing immediately prior to the start of the Term or created by the Contractor outside of the scope of the Services or this Agreement ("**Pre-Existing Material").** Further, notwithstanding anything else in this Agreement, the Contractor is permitted to re-use for its own business purposes any general know-how and techniques learned by and retained in the memory of the Contractor's Representatives as a result of the performance of the Services (excluding any Manitoba Confidential Material).

10.5 The Contractor grants to Manitoba a perpetual, irrevocable, non-exclusive, world-wide, royalty free licence to use, reproduce, modify, create derivative works from, display, publish and distribute internally and (subject to the subsections (a) and (b) below) externally the Pre-Existing Materials but only as part of the Work Product. This license includes the right of Manitoba to permit third parties to use the Pre-Existing Materials on condition that:

(a) the Contractor's copyright notices are clearly identified with the Pre-Existing Materials; and

(b) the third parties are obligated to use the Pre-Existing Materials solely for providing services to or on behalf of Manitoba.

10.6 The Contractor waives, and shall have each of its Representatives waive, all of their respective moral rights under the *Copyright Act* (Canada) in the Deliverables in favour of Manitoba, and the Contractor shall execute, or cause to be executed, any additional documents as may be required to evidence these waivers.

10.7 Any equipment, materials, and supplies provided by Manitoba to the Contractor for use in the performance of this Agreement will remain the property of Manitoba and will be returned without cost to Manitoba upon request.

10.8 The Contractor will retain ownership of, and responsibility for, the underlying equipment, software, staffing and delivery of Services. The Contractor will be responsible for all aspects of Service maintenance or defective devices or components thereof.

11. NOTICES

11.1 Any notice under this Agreement must be in writing and will be sufficiently given if delivered or sent by courier or email or facsimile, and addresses to the parties' addresses noted on the first page.

11.2 If courier or delivery service is disrupted by labour controversy, notice shall be delivered or sent by email or facsimile transmission.

11.3 The date of receipt of any such notice shall be deemed to be the date of delivery, electronic mail or facsimile of such notice if served personally, sent by electronic mail or couriered on a Business Day or if delivered, sent by electronic mail or couriered outside of the Business Day, then the next Business Day.

12. NO ASSIGNMENT/SUBCONTRACTING

12.1 Neither party shall assign or transfer this Agreement or subcontract any of its rights or obligations under this Agreement without the other party's prior written consent. Manitoba consents to those subcontractors identified in the Statement of Work. Notwithstanding the foregoing, Manitoba may assign or transfer any of its rights or obligations under this Agreement to another Manitoba governmental or quasi governmental entity or organization by providing written notice of such assignment or transfer to the Contractor.

12.2 No assignment or transfer or subcontracting of any part of this Agreement will relieve the Contractor from any obligations under this Agreement, except to the extent that they are

properly performed by Contractor's authorized or permitted assignees, transferees or subcontractors.

12.3 This Agreement will be binding upon the successors and any permitted assigns of Contractor.

13. AUDIT

13.1 The Contractor will provide Manitoba, its Representatives and auditors, and regulatory bodies having jurisdiction over Manitoba, with access (including to Contractor's books and records, facilities, premises where the Services are provided) reasonably necessary to conduct audits to verify compliance with this Agreement.

13.2 Such audits will be conducted at reasonably convenient times during the Term.

13.3 The Contractor will promptly:

(a) respond in writing to any written observations made as a result of any such audit reasonably requiring a response, including any audit undertaken by auditors appointed by Manitoba, or the Contractor's internal or external auditors (to the extent related to the Services) and, and in any event, within fifteen (15) days of receipt of such observations;

(b) without prejudice to any rights and remedies Manitoba has in law or under this Agreement, including rights of termination, promptly, after receiving written notice thereof, correct any non-compliance with any provision of this Agreement; and

(c) reimburse Manitoba as applicable for the undisputed amount of any overcharges, or reissue any unpaid invoice containing an error identified in an audit report provided to the Contractor by Manitoba.

13.4 Except for audits conducted by the Office of the Auditor General or any other regulatory authority, any Manitoba Representative conducting an audit pursuant to this Section 13 must enter into a non-disclosure agreement with the Contractor in form and substance consistent with the confidentiality and non-use obligations provided for in Section 5, mutatis mutandis.

14. GENERAL

14.1 The Contractor is an independent contractor, and this Agreement does not create the relationship of employer and employee, or of principal and agent, between Manitoba and the Contractor or between Manitoba and any Representatives of the Contractor. The Contractor shall be responsible for any deductions or remittances in respect of its Representatives, which may be required by law.

14.2 Time shall be of the essence of the Agreement. No change to this Agreement shall be valid unless in writing and signed by both parties. This Agreement shall be governed by the laws of the Province of Manitoba (without reference to conflict of laws principles) and the courts of the Province of Manitoba will have exclusive jurisdiction to hear all matters related to this Agreement. This Agreement constitutes the entire agreement between the parties in respect of the subject matter hereof. There shall be no undertakings, representations or promises, express or implied in respect of the subject matter hereof, other than those contained in this Agreement.

14.3 Those sections that by their very nature are intended to survive the termination or expiration of this Agreement shall survive the expiration or termination of this Agreement, including:

(a) Section 4 - Fees

(b) Section 5 – Confidentiality, Security and Personal Information

(c) Section 6 – Liability and Indemnification

(d) Section 7 – Insurance

(e) subsection 9.3 – Effect of Termination

(f) Section 10 – Ownership of Manitoba Data, Deliverables and Equipment

(g) Section 13 – Audit

(h) Section 14 - General

14.4 If any provision of the Agreement is for any reason invalid, that provision shall be considered separate and severable from the Agreement, and the other provisions of the Agreement shall remain in force and continue to be binding upon the parties.

14.5 No provision of this Agreement shall be deemed waived and no breach or omission excused, unless the waiver is in writing and signed by the party granting the waiver. A waiver of a term or condition of this Agreement in any regard shall not constitute a waiver or breach of any different or subsequent breach or omission.

Exhibit 1 – Protection of Personal Information

Definition of Personal Information

1.01 In this Exhibit and in this Agreement, "**Personal Information**" has the meaning given to that term in *The Freedom of Information and Protection of Privacy Act* of Manitoba (C.C.S.M. c. F175), and includes:

- personal information about an identifiable individual which is recorded in any manner, form or medium.

The requirements and obligations in this Exhibit:

(a) apply to all Personal Information received, collected or otherwise acquired by the Contractor in the course of carrying out its obligations under this Agreement, in whatever manner, form or medium;

(b) apply whether the Personal Information was received, collected or acquired before or after the commencement of this Agreement; and

(c) continue to apply after the termination or expiration of this Agreement.

Collection of Personal Information by the Contractor

1.02 The Contractor recognizes that, in the course of carrying out its obligations under this Agreement, the Contractor may receive Personal Information from Manitoba and may collect, acquire, be given access to and may otherwise come into possession of Personal Information about individuals.

1.03 Where the Contractor receives, collects, acquires, is given access to or otherwise comes into possession of Personal Information, the Contractor shall collect only as much Personal Information about an individual as is reasonably necessary to carry out the Contractor's obligations under this Agreement.

Restrictions respecting use of Personal Information by the Contractor

1.04

(a) The Contractor shall keep the Personal Information in strict confidence and shall use the Personal Information only for the purpose of properly carrying out the Contractor's obligations under this Agreement and not for any other purpose.

(b) The Personal Information shall be used solely by Contractor personally, or (where the Contractor is a corporation, business, organization or other entity) by the officers, employees and subcontractors of the Contractor, except as otherwise specifically permitted by Manitoba in writing.

(c) The Contractor shall:

(i) limit access to and use of the Personal Information to those of the Contractor's officers, employees and subcontractors who need to know the information to carry out the obligations of the Contractor under this Agreement,

(ii) ensure that every use of and access to the Personal Information by the Contractor and by the authorized officers, employees and subcontractors of the Contractor is limited to the minimum amount necessary to carry out the obligations of the Contractor under this Agreement, and

(iii) ensure that each officer and employee of the Contractor who has access to the Personal Information is aware of and complies with the requirements, obligations and fair information practices in this Exhibit, and

(iv) ensure that each officer and employee who has access to the Personal Information signs a pledge of confidentiality, satisfactory in form and content to Manitoba, that includes an acknowledgement that he or she is bound by the Contractor's privacy and security policies and procedures and is aware of the consequences of breaching any of them.

Restrictions respecting disclosure of Personal Information by the Contractor

1.05 Except as otherwise set out in this Exhibit, the Contractor shall not give access to, reveal, disclose or publish, and shall not permit anyone to give access to, reveal, disclose or publish, the Personal Information to any person, corporation, business, organization or entity outside the Contractor's organization, except as follows:

(a) to Manitoba, and to Manitoba's officers, employees and agents, for the purposes of this Agreement;

(b) to the individual the Personal Information is about, upon satisfactory proof of identity;

(c) where disclosure is required by legislation;

(d) where disclosure is required by an order of a court, person or body with jurisdiction to compel production of the Personal Information or disclosure is required to comply with a rule of court that relates to the production of the Personal Information; or

Protection of the Personal Information by the Contractor

1.06 The Contractor shall protect the Personal Information by putting in place reasonable security arrangements, including administrative, technical and physical safeguards, that ensure the confidentiality and security of the Personal Information and protect the Personal Information against such risks as use, access, disclosure or destruction which are not authorized under this Exhibit. These security arrangements shall take into account the sensitivity of the Personal Information and the medium in which the information is stored, handled, transmitted or transferred.

1.07 Without limiting subsection 1.08 of this Exhibit:

(a) where Personal Information is in paper form, or other removable media, the Contractor shall ensure that:

(i) the paper records and removable media used to record the Personal Information are kept in a physically secure area and are subject to appropriate safeguards, and

(ii) the paper records and removable media used to record the Personal Information are stored securely when not in use;

(b) where Personal Information is stored in electronic format, the Contractor shall:

(i) ensure that the computer system or computer network on which the Personal Information is stored is secure and is accessible only to officers, employees and subcontractors of the Contractor who need to know the Personal Information to carry out the obligations of the Contractor under this Agreement,

(ii) ensure that the Personal Information is protected by a series of passwords to prevent unauthorized access, and

(iii) limit access to and use of these passwords to those of the Contractor's officers, employees and subcontractors who need to know the Personal Information to carry out the obligations of the Contractor under this Agreement.

1.08 When disposing of any paper records and media containing a record of the Personal Information, the Contractor shall destroy the paper records or erase or destroy any Personal Information contained on the media in a manner which adequately protects the confidentiality of the Personal Information.

1.09 The Contractor shall establish and comply with written policies and procedures respecting the use of, access to, disclosure, protection and destruction of the Personal Information which shall be consistent with the requirements of this Exhibit. These security policies and procedures shall include:

(a) provisions for identifying and recording security breaches and attempted security breaches; and

(b) corrective procedures to address security breaches.

1.10 The Contractor shall, promptly upon becoming aware of any of the following, notify Manitoba in writing of any use of, access to, disclosure or destruction of Personal Information which is not authorized by this Exhibit, with full details of the unauthorized use, access, disclosure or destruction. The Contractor shall promptly take all reasonable steps to prevent the recurrence of any unauthorized use, access, disclosure or destruction of the Personal Information and shall notify Manitoba in writing of the steps taken.

1.11 The Contractor shall provide training for its officers and employees about the Contractor's security policies and procedures.

Inspections by Manitoba

1.12 Manitoba and its Representatives may carry out such inspections or investigations respecting the Contractor's information practices and security arrangements as Manitoba considers necessary to ensure the Contractor is complying with the terms and conditions of this Exhibit and that the Personal Information is adequately protected. The Contractor shall co-operate in any such inspection or investigation, and shall permit Manitoba and its Representatives access, at all reasonable times, to the Contractor's premises and to records and information relating to the Contractor's information practices and security arrangements or to this Exhibit for these purposes.

1.13 If an inspection or investigation identifies deficiencies in the Contractor's information practices or security arrangements which expose the Personal Information to risk of unauthorized use, disclosure or destruction, the Contractor shall take reasonable steps to promptly correct the deficiencies to Manitoba's satisfaction.

1.14 Except for audits conducted by the Office of the Auditor General or any other regulatory authority, any Manitoba Representative conducting an inspection or investigation pursuant to Section 1.12 must enter into a non-disclosure agreement with the Contractor in form and substance consistent with the confidentiality and non-use obligations provided for in Section 5, *mutatis mutandis*.

Exhibit 2

Estimated costs include:

Salesforce Outbound Dialer	18(1)(b) & 28(1)(b)
Training Development (our trainer time)	

17(1) & 17(3)(e)

KPMG Consultation	18(1)(b) & 28(1)(b)
KPMG Training Support	
Implementation fee	
Salesforce	
Salesforce Set Up	
Salesforce/Avaya CTI	
Reporting Development	

[redacted]

FIRST AMENDING AGREEMENT

First Amending Agreement (this "**Amending Agreement**") dated November 24, 2020 between the Government of Manitoba ("**Manitoba**"), 6th Floor-352 Donald Street Winnipeg, MB R3B 2H8, email: Gary.Luedtke@gov.mb.ca and 24-7 Intouch Inc. ("**Contractor**"), [redacted]

RECITALS:

(a) Manitoba and Contractor have entered into a services agreement dated April 13, 2020 for the provision of certain contact centre services and concurrently with the execution of this Amending Agreement a statement of work under such services agreement for the provision of contact tracing services (collectively, the "**Agreement**"); and

(b) Manitoba and Contractor wish to amend the Agreement to extend the term of the Agreement.

In consideration of the above and for other good and valuable consideration, the parties agree as follows:

Section 1 Defined Terms.

Capitalized terms used in this Amending Agreement that are not defined in it have the meanings given to them in the Agreement.

Section 2 Amendments to the Agreement.

(1) Section 1 of the first page of the Agreement is deleted in its entirety and replaced with:

Term: This Agreement starts on April 13, 2020 and will continue until May 24, 2021, unless terminated earlier in accordance with the terms hereof or extended by Manitoba for up to two (2) extensions of three (3) months each on the same terms as in this Agreement, in each case, by Manitoba providing at least 30 days' prior written notice to the Contractor of its intention to do so (the "**Term**").

Section 3 Reference to and Effect on the Agreement.

On and after the date of this Amending Agreement, any reference to this Amending Agreement in the Agreement and any reference to the Agreement in any other agreements will mean the Agreement as amended by this Amending Agreement. Except as specifically amended by this Amending Agreement, the provisions of the Agreement remain in full force and effect.

Section 4 Successors and Assigns.

This Amending Agreement becomes effective when executed by all of the parties. After that time, it will be binding upon and enure to the benefit of the parties and their respective successors, legal representatives and permitted assigns.

Section 5 Counterparts.

This Amending Agreement may be executed in any number of counterparts, each of which is deemed to be an original, and such counterparts together constitute one and the same instrument. Transmission of an executed signature page by facsimile, email or other electronic means is as effective as a manually executed counterpart of this Amending Agreement.

The parties have executed this Amending Agreement.

GOVERNMENT OF MANITOBA

By 17(1) & 17(3)(e) [redacted]

Title: Secretary to Treasury Board

By: _____

Name:

Title:

24-7 INTOUCH INC.

17(1) & 17(3)(e) [redacted]

Name: Mitul Kotecha

Title: President

By: _____

Name:

Title:

Schedule C - Statement of Work (SOW)
Dated April 15, 2020
to the Call Centre Agreement
Between 24-7 Intouch Inc. and the Government of Manitoba

This SOW is made as of April 15, 2020 (the “Effective Date”), pursuant to the terms of the Call Centre Agreement (the "Agreement") between the Government of Manitoba ("Manitoba") and 24-7 Intouch Inc. ("Contractor") dated April 13, 2020 for good and valuable consideration, the adequacy and receipt of which are hereby acknowledged by the parties hereto, the parties hereto agree as follows:

SECTION I – GENERAL TERMS

As provided for in the Agreement, this SOW comprises an integral part thereof. All capitalized terms not defined in this SOW shall have the meanings ascribed to them in the remainder of the Agreement (the “Remainder of the Agreement”). Notwithstanding anything contained herein, if a provision of this SOW specifically references a provision in the Remainder of the Agreement and provides that the provision of this SOW shall control in the event of a conflict, then such provision in this SOW shall control. For clarity, the only Sections of this SOW which shall override Schedule B of the Agreement are Sections IV(3)(f) and VI(1)(b) of this SOW. Any changes or additions to the services described herein or any other terms hereof shall first be mutually agreed upon and included as a Change Order to this SOW.

SECTION II – SERVICE SOLUTION

1. Contractor will deliver the services described in this SOW including, but not limited to, all customer engagement activity with dedicated agents (*defined as agents working only on the Manitoba program and are not shared with any other Contractor customers or partners*) for inbound and outbound voice interactions to support a list of approximately 65,000 Stakeholders applying for funding for the wage subsidy programs and the line of credit program associated with COVID-19 relief efforts of the Government of Canada and any other COVID-19 related government support programs requested by Manitoba from time to time (collectively, the “Programs”).

2. **Intentionally Deleted.**

3. Contractor and Manitoba mutually agree that customer interactions include:

    a. Outbound calls to inform Stakeholders about the Programs:
        i. Initial reach out to Stakeholders letting them know that the Programs exist.
            1. Manitoba will provide prioritization of industry/sector to determine the appropriate calling order and recontact rate.
            2. Contact will include scripting that references:
                a. That a Stakeholder *may* qualify for the Programs; and
                b. That the Contractor’s agents can help the Stakeholder to find the supports it needs.
            3. Continuous outbound calling on a cycle/pattern, to be mutually developed based on priorities, to ensure maximum coverage of call lists.
        ii. Continue outbound calling to track and understand who’s been successful in getting the support they need.
            1. Outbound reminders to re-submit for monthly wage subsidy.
            2. Outbound reminders to offer support and capture information re: submission success.
        iii. All outbound calls may be accomplished by leaving a scripted voicemail if a live answer is not received.

    b. Inbound call support to inform Stakeholders about the Programs

i. Provide guidance on how to fill out the forms.
ii. Provide information around changes as the Government of Canada may change the methods or processes to apply for funding.

iii. Multiple types of Stakeholders:
    1. Handled by Tier 1 – A Stakeholder who can do this by themselves. May not realize the Programs exist. They're tech savvy and can submit on their own.
    2. Handled by Tier 1 - Helping someone with reasonable tech savviness. Needs help on what data they need and explaining what the fields are.
    3. Transferred to Tier 1 Specialists - Not tech savvy and not comfortable navigating the Programs.
        a. e.g. how to open a myCRA account.

4. Hours of Operation
    a. Outbound calling: 9:00am-8:00pm weekdays and 10:00am-6:00pm on Saturdays, Sundays, and holiday days.
    b. Inbound calling: 6:00am-8:00 pm 7 days/week, with option to execute voicemail or queued callbacks from 8:00pm-9:30pm on weekdays.
    c. A minimum of three (3) Full Time Equivalent agents (FTE's) will be scheduled per language, English and French, for every given interval; an interval is defined as any 30 minute window within the scheduled hours of operation.

5. In accordance with Section 12.1 of Schedule B to the Agreement, the Contractor may leverage the following approved subcontractors:

    a. Five9; and
    b. Salesforce.

6. Contractor shall implement the Services, as contemplated in, and in accordance with, the transition plan attached hereto as Exhibit A (together with the Set Up Services (as defined in the Agreement), the "Implementation Services"). The Implementation Services shall be completed no later than within one month from the date hereof.

SECTION III – TECHNOLOGY SOLUTIONS

1. Telephony Solution

a. The Contractor will provide all communications circuits and toll-free numbers which will route calls to Contractor provided DIDs. Contractor will transfer the applicable responsible organization ownership to Manitoba as soon as reasonably practicable (and in any event before the end of the Term).
b. Manitoba will retain all inbound long-distance telco charges associated with Manitoba-owned toll-free numbers.
c. Contractor will be responsible for supplying and configuring the ACD ("switch") to route calls to agents once received at the Contractor system boundary. This includes configuration of skills, hours of operations, and IVR.
d. Contractor will be supporting Manitoba calls originating from customers in Canada.

2. Telephony Reporting

a. Contractor will provide access to a Manitoba-specific default enterprise reporting portal, including call center management metrics to support day-to-day operations and the periodic business review requirements.
b. Standard Reporting:
    i. ACD:
        1. Inbound Call Metric Reporting

a. Daily, Weekly, Interval, & Agent groups provided; historical data current within 15 minutes.

2. Outbound Call Metric Reporting
   a. Daily & Agent groups provided; historical data current within 30 minutes.
3. Queue Status Reporting
   a. Overview of calls in queue and various agent statuses for the purpose of queue management; blend of real time data current within 30 seconds as well as historical current within 15 minutes.

ii. Disposition:

1. Disposition Report
   a. Real time overview of disposition usage for the account.
2. Disposition Interval Statistics
   a. Real time overview of disposition usage by interval and date with graph and filter options.
3. Agent Disposition Statistics
   a. Historical data current within 15 minutes; provides disposition % and usage by agent.
4. Agent Disposition Detail
   a. Historical data current within 15 minutes; provides individual call records, limited metrics, and disposition.

c. Reports will be made available 24/7 via web portal and will provide cumulative information for 15-minute intervals.

3. Software Solutions

a. Contractor and Manitoba agree all tools and connectivity will be provided according to the following structure:

TECHNOLOGY	NAME OF SYSTEM	RESPONSIBILITY
CRM	Salesforce	Contractor
Email	Salesforce	Contractor
Call Center Software	Five9	Contractor
IVR	Five9	Contractor
Conferencing	Google Hangouts/Meet, Zoom, GoToMeeting	Contractor

4. Software Reporting

a. Stakeholder outcomes, including success or failure in accessing needed supports;
b. Quantification of supports received by Stakeholders;
c. Reasons for failures to access needed supports; and
d. Reporting will be with respect to the following data points:
   i. Business Name
   ii. Phone Number
   iii. Contact Name
   iv. Email Address
   v. Location of Business – Physical address
   vi. Type of Business (Category/Industry)

vii. How long in business - could be a disqualifier if not in business long enough
viii. Number of Employees prior to COVID
ix. Current Number of Employees
x. Has the business already laid employees off?
xi. If approved for a Wage Subsidy Program does the business plan on hiring employees back? – (Skip if they haven't laid people off)
xii. Annual Gross Revenue
xiii. Annual Gross Payroll (as identified on 2019 T4 Summary they would have submitted to CRA)
xiv. Program(s) interested in (pick from checklist, multiple - Wage Subsidy (10%), Wage Subsidy (75%), Line of Credit)
xv. Application Status for each specific program interested in (capture independently for each wage subsidy and line of credit)
    1. Have Not Applied
    2. Have Applied - When
    3. Have received funds
xvi. Follow up Required – Yes or No with qualification of why/for what
xvii. Any other data points reasonably requested by Manitoba

5. IVR Solution

a. Contractor will provide basic call treatment in the IVR to route calls within the Contractor switch as required. (ex. "For English, press 1; for French, press 2", etc.)
b. Due to speed of launch, Manitoba may choose to provide all or certain recordings required for the basic IVR setup in English and French. If Manitoba does not provide such recordings, such records shall be provided by Contractor. Scripts are subject to Manitoba's approval.
c. If additional voice recordings are required following initial launch, Contractor and Manitoba may create a Change Order (using the form in Schedule B attached to this SOW) and mutually agree on all costs associated with the change.

6. Workstation Specifications

a. Network LAN environment of 100MB / 1GB switches with VLAN capability.
b. Operating system Microsoft Windows 10 or Chrome OS.
c. Desktop systems use Windows 10 or Chrome OS.
d. Internet browser software to be configured within the requirements of Contractor ITSEC and (if required) PCI compliance.
e. Contractor will provide an appropriate computer or thin client, monitor(s), mouse and keyboard for agent and leadership workstations.
f. Contractor Network accessed from home workstations via VPN with dual factor authentication
g. Contractor will provide Jabra BIZ 1500 headsets (or an equivalent substitute) for voice agents.

7. Contractor shall provide the Services in accordance with the security requirements set out in Exhibit B to this SOW. Notwithstanding anything to the contrary, to the extent there is a conflict with Exhibit B and any other portion of this Agreement, Exhibit B shall prevail.

SECTION IV – STAFFING SOLUTIONS

1. Recruiting and Hiring

a. Contractor will develop an agent profile for recruiting and hiring purposes based on Manitoba's needs.
b. Contractor will ensure all candidates possess the adequate combination of skill set and cultural alignment to conduct the Services.
c. Contractor will deploy standard recruitment strategies to recruit agent candidates in accordance with local labor laws to meet all minimum requirements of the agent profile.
d. Contractor will implement a recruitment process that will include a combination of the following:

i. Internal transfers from other lines of business.
ii. Initial screening for high level fit, availability, and communication skills.
iii. Computer testing for grammar, spelling, English and/or French language comprehension, and computer skills.
iv. Home office suitability assessment, including geographic location, access to internet speeds, home office space requirements and program-specific technical requirements.
v. Face-to-face interview for general fit and selection criteria with a member of the Contractor's recruiting team, performed virtually or on-campus.
vi. Contractor will complete (or will have completed in the 12 month period prior to the Effective Date) Criminal Background Checks on all personnel providing Services which shall include at minimum a Canadian Criminal Background Check that includes the RCMP National Repository of Criminal Records.
    1. Due to COVID-19 related service interruptions, Contractor's responsibility to conduct background checks may in some cases be limited to due diligence of information reasonably available.

e. Contractor will commit to a recruiting and hiring cadence that meets all forecasted scheduling demands, outlined in Section IV(3), as required by Manitoba.
f. Subject to Section 3.3 of Schedule B of the Agreement, Contractor retains all final hiring or removal decisions on all personnel assigned to Manitoba.
g. Subject to the Contractor's internal Employee Handbook policies, Contractor confirms that new agents will not be eligible for internal transfers to another line of business until they have met their 90 day tenure mark and internal performance criteria.
h. Notwithstanding anything to the contrary, Contractor shall comply with all of the social distancing and other COVID-19 guidance published by the Government of Canada and/or the Province of Manitoba during the COVID-19 pandemic in connection with the provision of the Services.

2. Training

a. Contractor will utilize the support of pre-approved accounting professionals to build applicable training materials, to be reviewed and approved by Manitoba prior to use. For the purposes of this SOW, Manitoba approves KPMG as an accounting professional.
b. Contractor will provide all necessary virtual training environments. This may include virtual classrooms and self-led learning LMS, as needed to onboard agents to the Services.
c. Contractor will assign a trainer to be responsible for overseeing, supporting, and graduating agents during their virtual training and nesting period.
d. New hire training for all required headcount will be billed at the applicable paid hour rate outlined in the Cost Schedule (Section VI).
e. If Manitoba makes a change to process or an update to the product offering that requires additional training, Contractor will, if agreed in the applicable Charge Order pursuant to which the changes to process or product offerings have been agreed to by the parties, bill for all process or update training at the agreed upon paid hour rate.
f. Any up-training required by Manitoba will be billed back at the agreed paid hour rate.
g. Contractor will assume costs for new hire training attrition up to a maximum of 3 days of training per FTE (24 hours); "attrition" is defined as the replacement of existing agents who have quit, are terminated, promoted or otherwise taken off the Manitoba account.
h. If travel is required and pre-approved in writing by Manitoba for any Contractor training resource, Contractor will invoice Manitoba for all costs associated with travel.
i. For any additional headcount brought on to increase the size of the team, Contractor will provide new hire training at the agreed upon paid hour rate; additional headcount is defined as any agent being hired for purposes of supporting additional volume or right-sizing to support realized volumes.
j. Subject to subsection (g) of this Section, Contractor will cover all costs for new hire attrition training following graduation of any new hire training classes for team size growth.

3. Staffing and Schedule Planning

a. Contractor will use its own workforce technology for internal scheduling activities related to the deployment of the Services.
b. Contractor and Manitoba agree that staffing will be based on a mutually agreed upon Full Time Equivalent (FTE) target, developed by Contractor using all available inputs. The initial FTE targeted for production as soon as possible is 100 FTE (90 English and 10 bilingual French/English).
c. Manitoba will provide a project budget target broken down into monthly segments (ie. budgeted monthly spend) immediately following the execution of this SOW.
    i. Manitoba will provide a rough monthly budget forecast three months in advance and an updated monthly budget forecast one month in advance (e.g., the rough forecast for April will be provided the first business day of January). If Manitoba revises the budget (to increase or decrease its spend), Contractor will provide adjusted staff plans as required. In no event shall Contractor exceed the budget provided by Manitoba without Manitoba's prior written approval.
    ii. Should Manitoba need to update the monthly budget or the agreed upon Full Time Equivalent targets within the budget period based on business needs, Contractor will make best efforts to match the change. Should overtime be required and pre-approved by Manitoba in writing, Manitoba will be responsible for this cost (for greater certainty, as set out in Section VI). Contractor will provide weekly staffing forecasts based on Manitoba provided data for the locked, stretch and directional budget forecast period.
d. On a weekly basis, Contractor will provide staffing forecasts based on budget. Where contact forecasts or details on media events that may influence volumes are provided, Contractor will include said inputs and desired SLAs into the staffing model.
e. Contractor and Manitoba agree that any target service level metrics as outlined in Schedule A attached to this SOW shall be considered best effort.
f. In the event that the FTE requirements hereunder exceed 100 FTEs, the sixty (60) day notice period referred to in Section 9.1 of Schedule B of the Agreement shall be increased to fourteen (14) weeks.
g. Any changes to forecasting or scheduling requirements outside the scope of this SOW must be mutually agreed upon and included as a Change Order to this SOW.

SECTION V – OPERATIONAL DELIVERY

1. Quality Assurance

a. Contractor will develop a quality scorecard for the purpose of quality management and calibrations that reflects the goals of the program's Key Performance Indicators (for greater certainty, as set out in Schedule A attached to this SOW).
b. Contractor will monitor agent performance quality by listening to calls and evaluating any written forms of communication (e.g. emails, case notes, etc.).
c. Contractor will monitor a minimum of five (5) transactions for each agent monthly.
d. Contractor and Manitoba will participate in weekly calibration sessions, where both teams. collaboratively score interaction samples to ensure alignment on overall quality metric and strategy. If Manitoba does not participate in regular calibration calls, the Key Performance Indicators (for greater certainty, as set out in Schedule A attached to this SOW) shall become inapplicable.
e. Contractor will, at no additional cost to Manitoba, provide real time coaching and ongoing training to ensure maintenance of knowledge investment and follow through on actionable items.

2. Operational Resources

a. Contractor shall assign the following operational support model as soon as reasonably possible in accordance with the Transition Plan; any change to the support model or ratios will be tracked as a Change Order.

b. The amount of time a shared resource spends on the account will be determined based on the needs of the business work activity required as agreed to by both Contractor and Manitoba:
    i. Implementation Manager (for launch phase)
    ii. Agents - dedicated
    iii. Subject Matter Expert - dedicated; as needed on the program
    iv. Team Leader - 1:15 Ratio, dedicated
    v. Quality Analyst – 1:25
    vi. Dialer Operator – 1 dedicated
    vii. Trainer – 1:100, may be shared across multiple trainers
    viii. Operations Manager – 1:90, 1 dedicated
    ix. Director of Operations – 1:250
    x. For significant swings in volume, Team Leader ratios may need to be adjusted upon mutual agreement between Manitoba and Contractor
c. The following roles will be considered Key Personnel:
    i. Operations Manager
    ii. Program Leader

3. Meetings and Communication

a. The Contractor will meet with key stakeholders on the Manitoba team on a regular basis to review program performance (including service metric achievement) and discuss new solution recommendations. Frequency and topics are defined flexibly as follows:
    i. A weekly operations call of approximately 1 hour in length, attended by Manitoba's representatives. Additional attendees (e.g. Quality Analyst, Team Leader, Director of Operations) may be included based on meeting topics. Once per month, the weekly operations call will provide a monthly summary.
    ii. A monthly business review to discuss innovation and strategy roadmaps to enable ongoing achievement of cost reductions, process and operational efficiencies reflected in the service metric standards, expected to be approximately 2-4 hours in length, and attended by Manitoba's primary Operations and Leadership resources. Additional attendees may be included based on meeting topics. Meetings will be remote via web conference or conference call, or on-site at a Contractor campus.
b. Preapproved costs (in writing) for travel required by Manitoba for meetings above and beyond those described will be billed at cost and passed through to Manitoba.

4. Infrastructure

a. At-home workstations will adhere to Contractor's telecommuting policies including:
    i. Telecommuting Policy; and
    ii. Telecommuting Agreement.

    Any such policies shall be consistent with industry standards in all material respects.
b. Contractor will provide and maintain sufficient facilities, hardware and materials for the scope of the services, along with covering expectations on Manitoba growth within the Term.
c. Notwithstanding anything in the Remainder of the Agreement (including, for greater certainty, Section 3(a)(iii) of Schedule A), phone number data used in connection with the provision of the Services may be routed outside of Canada.

In connection with providing the Services, the Contractor will comply with its information security policies, which shall be consistent with industry standards in all material respects.

5. Language Support

a. All support will initially be conducted in English and French.
b. Additional language FTEs available upon request; costs to be mutually agreed upon and outlined by both parties as a Change Order to this SOW.

6. Change Order Process

a. In the event that the parties desire or are otherwise required pursuant hereto to change any of the terms of this SOW, the parties shall execute a Change Order (in the form attached as Schedule B hereto) providing for same.
b. Each Change Order will clearly state the implications to the project regarding deliverables, timelines and budget. No work identified on the Change Order will proceed without prior approval from each of the parties.

SECTION VI – COST SCHEDULE

1. Costs

a. In consideration for the Services, Manitoba shall pay to the Contractor the applicable fees set out below in accordance with the terms of the Agreement. Contractor shall not exceed Manitoba's provided monthly budget without Manitoba's prior written approval.

b. Notwithstanding anything contained in the Agreement (including this SOW), the Contractor shall not be required to provide any services hereunder or meet any applicable FTE target to the extent that doing so would result in the Contractor exceeding any budget provided by Manitoba pursuant hereto (unless Manitoba has provided its prior written approval in respect of such exceedance). For greater certainty, in the event that the Contractor does not provide any such services or meet any such FTE targets in the foregoing circumstances, such failures shall not be deemed or construed to be or result in a breach of any provision of the Agreement (including this SOW) provided that Contractor promptly notifies Manitoba in the event it suspects that the budget provided by Manitoba will impact its ability to provide any services hereunder or meet any applicable FTE target.

c. Contractor's pricing methodology was built based on an assumption of a minimum monthly total of 16,000 billable hours per month (100 Full Time Equivalent agents). Should the number of billable hours per month:

   i. fall below 8,000 (50 FTE) for more than three (3) consecutive weeks, or
   ii. increase above 24,000 (150 FTE),

   Contractor and Manitoba shall amend the pricing to equitably reflect the lower or higher volume (as applicable) and the dedication of resources identified in Section V, 2.

d. Contractor will invoice Manitoba on a monthly basis with payment terms as set forth in Schedule B of the Agreement, based on the following cost schedule outlined below. All invoices should be sent directly to the contact identified in the Agreement.

e. All flow through costs shall be invoiced to Manitoba as incurred by Contractor without mark-up.

Recurring Pricing (CAD):	Rate	Unit of Measure	Notes
English Tier 1	18(1)(b) & 28(1)(b) [redacted]	Paid Hour	Contractor assumes all Tier 1, Tier 1 Specialist, and SME time spent training and performing services on Manitoba's behalf is billable. Manitoba will not be responsible for lunches or paid time off. Manitoba shall pre-approve in writing the use of any Subject Matter Expert
English Tier 1 Specialist		Paid Hour	
English Subject Matter Expert		Paid Hour	
French/English Tier 1		Paid Hour	

French/English Tier 1 Specialist	18(1)(b) & 28(1)(b)	Paid Hour	
French/English Subject Matter Expert		Paid Hour	
Overtime Premium		Paid Hour	30% premium on the Effective Hourly Rate. For clarity, no overtime shall be incurred unless pre-approved by Manitoba in writing. Overtime Premium will not be payable in the event that overtime is the result of the Contractor not meeting its applicable staffing commitment during the locked period.
New Hire and Up-Training		Paid Hour	100% of the Effective Hourly Rate
Attrition Training	N/A	Paid Hour	Contractor will assume all costs for attrition assuming 3 days of training per FTE.
Monthly Costs	**Rate**	**Unit of Measure**	**Notes**
Per Month (Fixed)	17(1) & 17(3)(e)	Per Month	Limited to flow-through of the followingFive9 licensing (assuming 100 licenses) at 18(1)(b) & 28(1)(b)
Salesforce Licenses		Per License per month	Applicable for any license over 100 for the initial 6 months of the contract (April 13-October 12, 2020), and for all licenses as of October 13, 2020 onward
Variable Costs	**Rate**	**Unit of Measure**	**Notes**
Local and Long Distance Rates (Outbound - Canada)	18(1)(b) & 28(1)(b)	Per Minute	Billed in 30 second increments. All calls are billed based on carrier connection made, regardless of agent connection to the call.
Local and Long Distance Rates (inbound - Canada)		Per Minute	Billed in 6-second increments. All calls are billed based on carrier connection made, regardless of agent connection to the call. Includes all time spent in IVR, queue, and connected to the agent.
Set Up Costs	**Rate**	**Unit of Measure**	**Notes**
All-in Set Up Fee	18(1)(b) & 28(1)(b)	One Time	Limited to the costs/rates specified on Exhibit C. Will be included in the first invoice delivered pursuant to the Agreement.
Optional Additional Rates	**Rate ($CAD)**	**Unit of Measure**	**Notes**
IT Development	18(1)(b) & 28(1)(b)	Hour	IT Development fees are based on any post launch IT development related to change management, ad hoc reporting, or additional programming that is not part of initial implementation; charges are incurred only after mutual written agreement of project scope and costs.
Chat Bot Development	TBC	TBC	Subject to additional discussion and scoping

*Contractor shall not exceed such amounts without Manitoba's prior written approval.

IN WITNESS WHEREOF, Manitoba and Contractor have each executed and delivered this SOW as of the Effective Date.

The Government of Manitoba	24-7 Intouch Inc.
By: _____	By: _____
Name: Paul Beauregard	Name: Greg Fettes
Title: Secretary to Treasury Board	Title: CEO
Date: April 16, 2020	Date: April 16, 2020

Schedule A to Statement of Work
Service Level Key Performance Indicators (KPIs)

Contractor will use best efforts to adhere to the following service levels in accordance with the table below. Should adjustments need to be made to such service levels, Manitoba and Contractor agree to review and mutually agree upon the required changes and include them as a Change Order to this SOW.

Key Performance Indicators Table				
INBOUND PERFORMANCE TARGETS - BEST EFFORTS				
Metric	**Target Goal**	**Measurement Window**	**Reported**	**Calculated**
Utilization	≥70%	Monthly	Daily	Utilization = (Total Productive Minutes + Available Time)/(Staffed Time-breaks)
Quality Score	≥70%	Monthly	Daily	Quality Score will be assessed against a mutually agreed upon scorecard and will be targeted at 70%
Abandonment	Less than 10% of all calls offered will be abandoned	Monthly	Daily	The total number of calls Abandoned during a Measurement Window, divided by the total number of calls offered to Contractor during the Measurement Window. “Abandoned” means a call of over 30 minutes in duration that is received by the Contractor ACD and terminated prior to being answered by an Agent.
OUTBOUND PERFORMANCE TARGETS - BEST EFFORTS				
Full List Coverage	65,000 attempts	By close Mon, April 27	Daily	Measured by the dialer comparing total quantity of phone numbers entered into the system against quantity of phone numbers on which a call has been attempted

Schedule B to Statement of Work
Change Order Form

The Change Order Form layout provided below is considered a reasonable facsimile of the actual form as of the time of this SOW's execution. It is expected that the exact form layout may evolve over time, although the types of inclusions and data collected within the form will remain intact.

COMPANY:			
PROJECT:		**PROGRAM:**	
REQUESTOR:		**EMAIL:**	

Contractor SPONSOR:		**EMAIL:**	
REQUEST DATE:		**EFFECTIVE DATE:**	
CHANGE ID:		**PRIORITY:**	
APPLICABLE MSA/SOW ID:			

CHANGE TO BE IMPLEMENTED

COST SCHEDULE		
Type	**$**	**Description/Notes**

CHANGE ORDER APPROVAL

THE PARTIES AGREE THAT THIS CHANGE ORDER SHALL BE MADE TO THE STATEMENT OF WORK (SOW), EFFECTIVE AS OF THE DATE SET OUT ABOVE. EXCEPT AS SPECIFICALLY MODIFIED BY THIS CHANGE ORDER, ALL TERMS AND CONDITIONS OF THE SOW REMAIN UNCHANGED AND IN FULL FORCE AND EFFECT. THIS CHANGE ORDER SHALL BE APPENDED TO THE SOW ONCE FULLY EXECUTED.

GOVERNMENT OF MANITOBA		**24-7 INTOUCH INC.**	
Signature:		**Signature:**	
Name:		**Name:**	

Title:		**Title:**	
Date:		**Date:**	

Exhibit A to Statement of Work

Transition Plan

Key Milestones

Manitoba

	04/12/20	05/10/20	
Recruiting			
Recruiting Dates	04/13/20	04/26/20	Ongoing, targeting internal hires to begin
Training			
Wave 1	04/15/20	04/15/20	Internal Agents
Wave 2	04/16/20	04/16/20	Internal Agents
Wave 3	04/20/20	04/20/20	Blend of Internal & External Hires
Wave 4	04/27/20	04/27/20	Blend of Internal & External Hires
IT Items			
Salesforce Configuration	04/13/20	04/17/20	Initial set up with ongoing configuration as needed
Telephony Configuration	04/13/20	04/17/20	Initial set up with ongoing configuration as needed
Production			
GO LIVE	04/16/20		Outbound & Initial Inbound Messaging
Uptraining and Increased Inbound Skill	04/20/20	05/03/20	Subject to release of Wage Subsidy information
Uptraining and Increased Inbound Skill#2	05/04/20	05/10/20	Subject to change. Development of Specialists and SMEs as required

Exhibit B to Statement of Work
Security Requirements

1. The Contractor must have implemented security procedures revoking physical card access to space; network credentials and access are suspended within 24 hours of termination of employment. This must include any subcontracting agreements or arrangements.

Relationships with Sub Contractors

1. The Contractor must disclose to Manitoba the use of sub contactors to satisfy Manitoba's requirements and must include details related to the capacity in which the subcontractor will be used for the delivery of services to Manitoba.

2. All changes to subcontracting arrangements must be made in writing and approved by Manitoba before applying them to service in support of Manitoba's requirements.

3. The Contractor must have documented, and provide to Manitoba upon request, how Manitoba requirements flow to all sub contactors and how requirements satisfaction is determined.

4. The Contractor must have documented, and provide to Manitoba upon request, what Manitoba information is shared with and used by sub contactors. This must include procedures in place for protecting this information.

5. The Contractor must ensure that security risks associated with sub contactors are defined and monitored.

Datacenter

1. The Contractors must identify the locations of the datacenters that will be used to deliver services to Manitoba.

2. The Contractor must identify if the datacenters used in the delivery of services are dedicated to the Contractor's services or if the Contractor leverages a shared data centre or a sub contracted datacenter provider. If shared the Contractor must secure Manitoba's data from other customers.

3. The Contractor must identify the certified Tier classification of the datacenter used to provide services to Manitoba as defined by the Uptime Institute (Tier 1-4).

4. The Contractor must have physical controls in place to control access to information assets and IT services and resources based on their importance including the approval process for the Identification and authentication of Contractor staff members who have physical access to assets providing Manitoba services including temporary access.

5. The Contractor must ensure protection from unauthorized physical access including Logging of physical access.

6. The Contractor must have documented, and provide to Manitoba upon request, a description the physical security attributes of the datacenter systems such as uninterruptible power supplies, backup generators, redundant climate control systems, card access systems, and a data-center-grade fire control system for prevention and protection.

7. The Contractor must maintain the physical security of the data center systems and they must be monitored, maintained and audited for proper operating efficiency.

Service Scalability

1. The Contractor must ensure the solution handles increased capacity demands such as sudden increases in capacity demands as result of an event impacting multiple clients leveraging your service ensuring Manitoba's services are maintained.

Contingency Planning; Operational and Disaster Recovery

1. The Contractor must have business continuity and disaster recovery (BC/DR) plans for critical assets and must be able to demonstrate that plans are tested on an annual basis. The Contractor must indicate if they completed self testing or if testing was completed by an independent third party.

2. The Contractor must have BC/DR plan and procedures applicable to the requested services and the site(s) where these services are operated

3. The Contractor must have BC/DR plans, including testing, for all sub Contractors involved in delivering the requested services.

Security Policies, Procedures, and Practices

1. The Contractor must exercise appropriate standards of due care with respect to securing information assets, primarily accomplished through security policies, procedures, and practices that are documented, auditable, enforced, reviewed and updated annually.

2. The Contractor must provide to Manitoba a completed SOC1, SOC2 Type 2 and PCI-DSS attestation and/or independent report as applicable, which was completed within the last 12 months or less.

3. The Contractor must agree to address any significant finding to the satisfaction of Manitoba.

4. The Contractor must have a comprehensive set of documented, current policies demonstrating how they are periodically reviewed, updated, audited and enforced.

Access Control

1. The Contractor must have access control policies which ensure that only duly authorized staff members who use and support requested service systems have access to the operating system, applications, and databases to be used in providing the requested services.

2. The Contractor must monitor and enforce all access control policies.

3. The Contractor must have access control policies enforced for all subcontractors who are engaged in the delivery of the services to Manitoba.

4. The Contractor must have access controls and processes for access request, access review, and access termination that are auditable.

5. The Contractor requires the use of at least two-factor authentication for staff and the use of encrypted virtual private networks for remote access into the Contractor network including any staff participating in any Work-At-Home programs or initiatives.

6. The Contractor must have policies that are enforced and monitored to ensure appropriate levels of user authentication and control of user access.

7. The Contractor must have policies that ensure development and operations staff have segregated roles and responsibilities.

8. The Contractor must ensure that developers are limited to the testing, training, and user acceptance testing (UAT) environments.

9. The Contractor must ensure that all users including administrators, super users, database administrators, etc. are uniquely identified at all times.

10. The Contractor must ensure that all system, process, or database passwords be changed from default settings, systems are locked if not in use, and passwords are changed a minimum of one time per year.

11. The Contractor must ensure that clear text passwords will not be transmitted across the network at any time.

12. The Contractor must implement a range of security controls to protect service systems and networks to include:

    a. Access controls at the level of networks, systems, files, and applications.
    b. Perimeter and internal firewalls that implement security policy.
    c. Network security monitoring in the form of intrusion detection or event monitoring.
    d. System disposal process that securely wipes all data prior to disposal.
    e. A means for client data, system, network, and performance protection from exposure to other clients when the service executes on shared servers or devices.
    f. That all the above processes are recorded and auditable.

Software Integrity

1. The Contractor must ensure the integrity of installed software by ensuring they are regularly checking for all viruses, worms, Trojan horses, and other malicious software and eradicating them in a timely manner.

2. The Contractor must ensure up-to-date virus signatures and other relevant signatures such as those for intrusion detection systems.

Secure Asset Configuration

1. The Contractor deployed and documented, using documented procedures and processes, secure configuration of all client information assets throughout their life cycle (installation, operation, maintenance, retirement) by addressing all items listed below.

2. The Contractor must ensure that all hardware and software used in the delivery of services to Manitoba are supported by the hardware manufacturer, or developer of the software components, used in the delivery of services.

3. The Contractor must ensure that a vulnerability management program is in place and that patches are applied to correct security and functionality problems.

4. The Contractor must ensure that vulnerability scans are performed on a monthly basis and new systems are scanned once implemented.

5. The Contractor must have , and provide upon request to Manitoba, their schedule for patching the software on service systems including a scheduled time periods for systems patches (i.e. a time period on a specific day of the week where routine, non-critical patches are applied to service systems) ensuring no interruption of services provided to Manitoba.

6. The Contractor must apply critical security patches on systems, firewalls, routers and switches within 30 days, or sooner, of release by supporting vendor.

7. The Contractor must provide Manitoba with a monthly report listing the patches applied.

8. The Contractor must have a standard including minimum essential configuration for each type of computer and each type of service, storing this as a trusted base configuration. The standard must include removing or disabling all unnecessary applications and services (producing a minimum essential configuration), removing default accounts, and patching known vulnerabilities.

9. The Contractor must have a process for securely configuring service systems prior to deployment, and for keeping the system security configuration up to date

10. The Contractor must identify which infrastructure components are shared in the delivery of the service to Manitoba.

11. The Contractor must test configurations in a non-production environment prior to deployment

12. The Contractor must have architectural diagrams of their solution with Manitoba and provide them upon request.

13. The Contractor must have configuration management and change control procedures including test procedures that are exercised when changes are made. This must include an ability to recover from upgrade and patch installation problems, a back out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.

14. The Contractor must allow Manitoba to approve changes, if warranted, and notification when changes are made that can affect Manitoba's service processing, performance, and data so that testing may be performed.

15. The Contractor must consider security during the implementation of all changes to Contractor's systems and networks.

16. The Contractor must have a process(s) for conducting penetration tests on a regular basis including steps demonstrating how weaknesses are addressed in a timely manner when identified.

17. The Contractor must ensure Manitoba that no undocumented, unreported configuration changes will occur to the service provided.

18. The Contractor must maintain a secure firewall configuration to Manitoba standards to isolate the System from the Contractor systems and from the Internet.

19. The Contractor must ensure that Firewall logging is enabled and reviewed through manual or automated tools.

20. The Contractor must have in place text and graphics, describing how your services will be implemented and must include a description as to how Manitoba data and the supporting systems including networking connections are protected from exposure to other clients.

21. The Contractor must have descriptions as to how you manage the systems and the supporting tools used as part of the provided services.

Monitoring:
The Contractor must monitor for, all systems used in the delivery of services to Manitoba:

1. Availability, performance and security in real time.

2. Ensure the monitoring team, Network Operations and IT operating have appropriate separation of duty designed into their reporting structure.

3. Minimum performance baselines.

4. All network traffic entering and leaving the network.

5. The entire network (firewalls, intrusion detection systems, routers, servers, niche security products, customer applications) including all core Infrastructure and relevant sensors. This must include interface state, throughput, packet loss, environmental, CPU, memory, fan speed of all physical hardware, power state.

6. That significant monitoring results are reported and actioned accordingly

7. Perform automated audit logging security related events, including individual access.

8. Ensure audit logs are accessible to authorized individuals, protected from unauthorized access, and periodically reviewed.

9. Upon request the Contractor must provide Manitoba with a report of the audit logs.

Breaches of Security

1. The Contractor must notify Manitoba immediately, in writing, of any security breach or attempted security breach with the potential to impact Manitoba's security or the security of confidential or sensitive Manitoba information maintained by the Contractor

2. The Contractor must identify what steps are being taken to prevent a recurrence and provide a root cause analysis for breaches of security.

Site Visit

1. The Contractor must grant access to Manitoba, or an authorized third party retained by Manitoba to conduct a site visit, at Manitoba's discretion, including all physical facilities involved in service delivery such as the datacenter where client data are secured.

2. The Contractor, during site visits, must provide reviews and demonstrations of Contractor capabilities as represented in the proposal. Manitoba may, at its discretion, provide additional scenarios or requirements that may be examined. These will be communicated in writing prior to such a visit. Expenses incurred by the Contractor during the site visit are the Contractor's responsibility.

3. The Contractor must specify any limitations or constraints on site visits.

Exhibit C to Statement of Work
Set Up Fees

Item	Set Up Cost	Notes/Description
Five9 Telephony	18(1)(b) & 28(1)(b)	Five9 Telephony. 18(1)(b) & 28(1)(b) for additional licenses 18(1)(b) & 28(1)(b) one-time cost for additional licenses
Training Development (our trainer time)		Assume 18(1)(b) & 28(1)(b) for initial build. Ongoing curriculum dev done by designated trainer; cost included
Training Consultation		Includes an initial development budget of up to 18(1)(b) & 28(1)(b) Any further consultation invoiced as a pass-thru cost as incurred.
Implementation fee		Covers implementation effort for short-term program
Salesforce		18(1)(b) & 28(1)(b) For every additional license, and all licenses beginning July 13, 2020, invoiced at a monthly cost of 18(1)(b) & 28(1)(b)
Salesforce Set Up		Includes 80 hours for our internal team for Salesforce set up and 50 hours of Salesforce consultation.
Salesforce/Five9 Integration		Integration of inbound dialer to execute “call pop” for agents with prior contact history and contact details
Reporting Development		Assumes 20 hours of reporting development time to build custom dashboards for visibility 18(1)(b) & 28(1)(b)

[redacted]

[redacted]

THIS EXTENSION AGREEMENT is made as of the 6th day of October, 2020.

BETWEEN:

GOVERNMENT OF MANITOBA
(hereinafter called "**Manitoba**")

OF THE FIRST PART,

- and –

24-7 INTOUCH INC.
(hereinafter called the "**Contractor**")

OF THE SECOND PART,

WHEREAS the Contractor and Manitoba are parties to a Call Center Agreement dated as of April 3, 2020 (the "**CCA**");

AND WHEREAS attached to the CCA are certain Statement Of Works ("SOWs") as follows:

(a) Schedule Statement of Work dated April 15, 2020 as amended by subsequent change orders

AND WHEREAS the parties are desirous of extending the term of the CCA as more particularly set out herein;

NOW THEREFORE in consideration of the mutual agreements set out herein, the parties agree as follows:

1. **Preamble.** The preamble hereto shall form an integral part hereof.

2. **Capitalized Terms.** All capitalized terms used herein shall, unless a contrary intention is expressed herein, have the same meaning as defined in the CCA or the SOWs.

3. **Extension to the CCA. By this Extension Agreement to the CCA the Contractor and Manitoba desire and agree to extend the term of the CCA in accordance with Section 1 (Term) for the first of two (2) extensions, for a period of three months commencing on October 12, 2020 until January 12, 2021 unless further extended in accordance with the CCA.**

4. **Other Terms and Conditions of the CCA.** The Contractor and Manitoba confirm that, in all other respects, the terms and conditions of the CCA and the SOW remain unchanged and in full force and effect, except as the CCA has been modified and supplemented by this Extension Agreement. For greater certainty, it is agreed that all other provisions of the CCA and the SOW shall be amended, *mutatis mutandis*, to give effect to the amendments as set out in this Extension Agreement.

26 [redacted]

[redacted] 17(1) & 17(3)(e)

5. **Enuring Effect.** This Extension Agreement shall enure to the benefit of and be binding upon the parties and their respective heirs, executors, successors, legal representatives and permitted assigns.

6. **Time is of the Essence.** Time is of the essence with respect to all matters for which a time period is prescribed in this Extension Agreement.

7. **Further Assurances.** The parties agree, from time to time, to do or cause to be done all such things, and shall execute and deliver all such documents, agreements and instruments reasonably requested by the other party, as may be necessary or desirable to carry out the provisions and intention of this Extension Agreement.

8. **Governing Law**. This Extension Agreement shall be construed and governed by the laws of the Province of Manitoba.

9. **Entire Agreement.** The CCA and the SOW, as extended by this Extension Agreement, represent the entire agreement between the parties, and there are no other agreements, promises or understandings, oral or written, between the parties in respect of this subject matter.

10. **Execution in Counterparts.** This Extension Agreement may be signed in multiple counterparts, each of which will be considered an original, and all of which will be considered one and the same document. Counterparts may be delivered either in original or faxed form or by way of a .PDF or similar scan attached to an e-mail and the parties adopt any such signatures received by a receiving fax machine or by e-mail as original signatures of the parties; provided, however, that any party providing its signature in such manner shall, if required at the request of the other party, promptly forward to the other party an original of the signed copy of this Extension Agreement which was so faxed or e-mailed.

IN WITNESS WHEREOF the parties hereto have caused this Extension Agreement to be properly executed on the day and the year first above written.

GOVERNMENT OF MANITOBA

17(1) & 17(3)(e) [redacted] Richard Groen

Date: OCT 2 9 2020

24-7 INTOUCH INC.

17(1) & 17(3)(e) [redacted]

Per: [redacted]

Nsme: Mitul Kotecha PresidentU

Date: Oct-16-2020

26 [redacted]

This statement of work (this "**SoW**") is between the Government of Manitoba ("**Manitoba**") 6th Floor-352 Donald Street Winnipeg, MB R3B 2H8, email: Gary.Luedtke@gov.mb.ca and 24-7 Intouch Inc. ("**Contractor**") 17(1) & 17(3)(e) [redacted] 17(1) & 17(3)(e) for the purchase of certain contact tracing services pursuant to the services agreement between the parties dated April 13, 2020 (the "**Service Agreement**").

WHEREAS:

A. On April 13, 2020, Manitoba and the Contractor entered into the Services Agreement for the provision of certain contact centre services; and

B. Manitoba and the Contractor wish to add additional services to the Services Agreement subject to the terms and conditions set out in this SoW.

NOW, THEREFORE, Manitoba and the Contractor agree as follows:

1.1 **Services Agreement.** Except as otherwise specified herein, this SoW is subject to the terms and conditions of the Services Agreement (including Schedule B) and forms part of the Services Agreement as Schedule C-2. Capitalized terms not otherwise defined in this SoW shall have the meanings attributed to such terms in the Services Agreement.

1.2 **Tracing Services.** The Contractor shall perform the services set out on Exhibit 1 hereto (the "**Tracing Services**"). Any reference to the "Services" in the Services Agreement shall be deemed to include the Tracing Services. The first paragraph of Section 2 of the Services Agreement entitled "Documents" is hereby amended as follows:

Documents: This Agreement is comprised of this first page and the following schedules:
(a) Schedule A – Services
(b) Schedule B - Terms and Conditions
(c) Schedule C -1 – Statement of Work for contact centre services entered into on April 13, 2020
(d) Schedule C -2 – Statement of Work for contact tracing services entered into on November 24, 2020

1.3 **Conflicts.** Notwithstanding anything to the contrary in the Services Agreement, to the extent there is a conflict between the terms and conditions of this SoW and the terms and conditions of the Services Agreement, the terms and conditions of this SoW shall prevail.

1.4 **Fees.** In consideration of the performance of the Tracing Services, Manitoba shall pay to the Contractor the fees specified in Exhibit 1. The payment of such fees are subject to Sections 4.3 through 4.6 of Schedule B of the Services Agreement.

1.5 Key Personnel. The following personnel shall constitute "Key Personnel" for the purposes of this SoW: Relationship Manager, Service Lead, Team Leads.

1.6 Privacy. In addition to the requirements set out in Section 5 (excluding Section 5.15) of the Schedule B to the Services Agreement, the Contractor shall use its Commercially Reasonable Efforts (as defined below) to:

(a) comply with the requirements respecting the collection, use, disclosure and destruction of Personal Information as set out in *The Freedom of Information and Protection of Privacy Act* (Manitoba) and *The Personal Health Information Act* (Manitoba), and the regulations to those Acts;

(b) execute the documents attached hereto as Exhibit 2 (the "**Information Management Agreement**") and Exhibit 3 (the "**Information Sharing Agreement**") and comply with the obligations provided therein; and

(c) comply with its obligations set forth on Exhibit 4 (Security).

1.7 **Deviations from the Services Agreement.** For the purposes of this SoW, the following shall apply:

(a) Section 3.2 (d) of Schedule B to the Services Agreement shall not apply to the Tracing Services.

(b) Section 5.15 of Schedule B to the Services Agreement shall not apply to the Tracing Services.

(c) Notwithstanding anything to the contrary in the Services Agreement, but subject to the last paragraph of this Section 1.7(c):

i. Manitoba acknowledges that the Services to be provided by the Contractor include calling Manitoba provided phone numbers, following a script provided by Manitoba, inputting answers gleaned from the individual who answered the call into Manitoba provided systems (e.g. PHIMS) for the purposes of COVID Contact Monitoring, Daily Follow Up and, to the extent agreed to by the parties, case investigation, and that correspondingly, except for certain call lists provided by Manitoba, the Contractor will not store or host Manitoba Data outside of Manitoba's environment and infrastructure; and

ii. provided the Contractor has utilized commercially reasonable efforts to comply with its obligations under this SoW and the Services Agreement in a manner consistent with industry practices applicable to leading providers of similar services ("**Commercially Reasonable Efforts**"):

1. Section 6.1 and Section 6.2 of Schedule B to the Services Agreement shall not apply to the Tracing Services except with respect to any software made available by the Contractor in connection with the provision of the Tracing Services;
2. the Contractor shall have no liability to Manitoba whatsoever as a result of or in connection with providing or failing to provide the Services in accordance with the terms of this SoW, the Services Agreement, the Information Management Agreement, the Information Sharing Agreement, and/or its obligations in Exhibit 4 (Security);
3. Manitoba hereby waives any and all breaches of this SoW, the Services Agreement, the Information Management Agreement, the Information Sharing Agreement and/or Exhibit 4 (Security) by the Contractor which may arise as a result of or in connection with the Contractor providing or failing to provide the Services; and
4. Manitoba shall indemnify, defend and save the Contractor harmless against, and will reimburse the Contractor for, any and all damages, losses, liabilities, costs and expenses that are suffered or incurred by the Contractor arising from or in connection with any claim by a third party:
    a. as a result of any security breach impacting, or loss of, Manitoba Data, or a breach of the Contractor's obligations under Section 1.7 (Privacy), the Information Management Agreement, the Information Sharing Agreement and/or Exhibit 4 (Security); and

b. alleging the Contractor's provision of, or failure to provide, the Tracing Services resulted in the injury, illness or death of any individual.

Notwithstanding the foregoing, in the event the Contractor, despite using Commercially Reasonably Efforts, fails to comply with any of its obligations, in any material respect,:

a. the Contractor's CEO shall meet with a Manitoba designated representative to explain why the Contractor was unable to comply with its obligations and propose a plan for remediation; and
b. Manitoba shall be entitled to terminate the Services Agreement and/or the Tracing Services for cause pursuant to Section 1.7(d)(ii).

(d) Section 9.1 and Section 9.2 of Schedule B to the Services Agreement shall not apply to the Tracing Services.

i. Manitoba may at any time terminate this SoW, or a portion of this SoW, for convenience on sixty (60) calendar days' notice in writing to the Contractor. In the event that such termination requires the Contractor to lay-off any personnel involved in the performance of the Tracing Services, Manitoba shall pay to the Contractor any out of pocket costs reasonably and actually incurred (i.e., no mark-up) by the Contractor to lay off such personnel, such costs not to exceed the following:

Number of Personnel to be Laid-Off	Fee
18(1)(b) & 28(1)(b) [redacted]	18(1)(b) & 28(1)(b) [redacted]

(the "**Termination For Convenience Fee**"). The Contractor shall use reasonable efforts to mitigate all costs incurred by the Contractor as a result of such termination including reassigning personnel. The Contractor shall: (a) notify Manitoba at the time of receiving the notice of termination of the expected number of personnel which Contractor expects to lay-off; and (b) provide Manitoba any information or documentation reasonably requested in order to substantiate the Termination For Convenience Fee. The Termination For Convenience Fee shall be the Contractor's sole and exclusive remedy for Manitoba terminating pursuant to this Section.

ii. Without restricting any other remedies available either party may immediately terminate this SoW with written notice if the other party has failed to comply with any material term or condition of this SoW and/or the Services Agreement, and has failed to remedy the failure within ten (10) Business Days following the receipt of the written notice of default.

[redacted]

1.8 **Counterparts.** This SoW may be executed in counterparts, each of which will be deemed to be an original of this SoW and tougher with constitute one and the same instrument. Delivery of this SoW (including an executed signature page) by electronic transition will be as effective as delivery of a manually executed copy of this SoW.

THIS SOW has been executed on behalf of Manitoba and the Contractor, by their duly authorized representatives, on the dates noted below.

[redacted]

ITOBA

Minister of [redacted] (or designate)

Name: Paul Beauregard

Date: November 24, 2020

24-7 INTOUCH INC.

DocuSigned by:

Per: [redacted]

Name: Mitul Kotecha

Nov-24-2020

Exhibit 1 to Schedule C2 - Statement of Work (SOW) No. 2 Contact Tracing

SECTION I – SERVICE SOLUTION

1. Contractor will deliver the Services described in this SOW including, but not limited to, public engagement activity to follow up on COVID cases with dedicated agents (defined as agents working only on the Manitoba program and are not shared with any other partners) via primarily voice based case management.

2. Contractor and Manitoba mutually agree that the Services include interactions comprised of, but are not limited to, the following Contact Types:
    a. Phase One: Activation to launch immediately upon execution of this SoW which shall include:
        i. Preparation of detailed activation plan for Contractor Services for:
            - Daily case and contact follow up
            - Daily case and contact monitoring
            - Case Investigation
        ii. Development of Resource Training Plan
        iii. Development of onboarding schedule with resource targets and milestones
        iv. Development of technology activation and support plan
        v. Definition of target service levels associated with delivery of each service by Contractor resources
        vi. Establishment of service oversight and management framework between Contractor and Manitoba
        vii. Confirmation of service reporting approach including performance metrics and KPIs
        viii. Finalization of service billing approach
        ix. All other activities necessary to activate Contractor's ability for delivery of full services contemplated by this SOW
        x. Where possible, Contractor will initiate delivery of Daily Contact Follow Up and Monitoring Services with an advance team up to 50 resources
    b. Phase Two: The following services shall be performed based on the schedule established in Phase One:
        - Daily case and contact follow up
        - Daily case and contact monitoring
        - Case Investigation
    c. Phase Three: Activation of call center management and support services to support Manitoba including:
        i. Assessment of opportunities to incorporate Contractor management and team lead resources into the Manitoba contact tracing team
        ii. Development and approval of resource plan and schedule
        iii. Confirmation of service delivery requirements and expectations
        iv. Establish a cost/price/budget for services to be documented in a new SOW

        Decisions to proceed with this service will be mutual based on the above activities. Manitoba and Contractor agree that this service is advisory in nature and that Contractor cannot be responsible for the performance or actions of third party resources.
        This service shall in no way be construed as employment or co-employment of such third party resources by the Contractor.

3. Contractor will use commercially reasonable efforts to achieve the service levels and key performance indicators outlined in Schedule A.

4. Language Support
   a. The Services will be conducted in English and French
   b. Manitoba and Contractor will determine best approach to align Contractor services with established simultaneous translation service as part of Phase One.

5. Hours of Operation
   a. The hours of operation for the Services shall be:

Day of Week	Opening	Closing
7 days per week	8:00am Central Time	8:00pm Central Time

This is inclusive of holidays. Hours of operation on any day, including holidays, may be adjusted with 30 days advance notice by Manitoba.

6. Contractor agents will perform the Services outlined herein to support the interactions and hours listed above. Any changes or alterations to the Services or requests for additional services shall be subject to the change order process and change order document.
   a. If Manitoba requests that Contractor perform any services that are:
      i. Materially different from the Services described above; or
      ii. Require materially different levels of effort, resources or expense from Contractor for which there is no current charging methodology in the applicable SOW ("New Services"), Contractor shall promptly prepare a solution for Manitoba's consideration.
   b. Manitoba shall provide such information as Contractor reasonably requests in order to prepare such New Service proposals.
   c. Manitoba may accept or reject any New Services proposal in its sole discretion and Contractor shall not be obligated to perform any New Services to the extent the applicable proposal is rejected. Unless the Parties otherwise agree, if Manitoba accepts Contractor's proposal, Contractor shall perform the New Services and be paid in accordance with the proposal submitted by Contractor and the provisions of the Agreement. The New Services shall be appended to this SOW via a signed Change Order in a mutually agreeable format.

SECTION II – TECHNOLOGY SOLUTIONS

1. Telephony Solution

   a. Contractor will be responsible for supplying and configuring the ACD ("switch"). This includes configuration of skills, hours of operations, and IVR, if deployed on the program.
   b. Contractor will be supporting Customer calls originating from and going to residents located in Manitoba, Canada.

2. Software Solutions

   a. Contractor and Manitoba agree all tools and connectivity will be provided according to the following structure:

i. Contractor will access all Manitoba provided technology via web-based logins via specified URLs
ii. Contractor agents shall log into Manitoba systems using a Manitoba-provided Multi-Factor Authentication token.
iii. Manitoba will provide all license access to Contractor for all Manitoba provided software listed below in advance of training; the timing to be mutually agreed upon during Phase One Activation planning

SOFTWARE	NAME OF SYSTEM	RESPONSIBILITY
Health Information Platform	Panorama, PHMIS	Manitoba
Call Center Telephony	Avaya	Contractor
Email	Microsoft Office	Manitoba
Multi-Factor Authentication Token	Provided by Digital Health	Manitoba
VPN for Remote Access	Cisco or equivalent	Contractor
Internet browser	Firefox, Chrome (both best compatibility)	Contractor
Workforce Management and Scheduling	Aspect	Contractor
Internal Chat (Agent/Leader)	TeamRooms	Contractor
Data Loss Prevention	ForcePoint	Contractor, pass-thru cost to Manitoba
Conferencing	GoToMeeting, Zoom)	TBD - as mutually agreed by Manitoba and Contractor

b. If Manitoba wishes to change any of the foregoing software at any time within the term of this SoW, a Change Order and Project Plan will be implemented to address any cost impacting changes

3. Software Reporting

a. Manitoba will be responsible for ensuring Contractor will have access to all necessary reports to manage agent performance.
b. KPIs outlined in Schedule A, whose management is dependent upon the reporting access described herein, shall not be enforceable until data visibility and system access is established.
c. Contractor shall provide standard outbound telephony reporting. Customization of this reporting shall be discussed and the work scope mutually agreed upon during Phase One Activation planning.

4. **Agent and Team Leader Workstation**
    a. Contractor shall provide each agent performing Services a workstation conforming with the following specifications:
        i. Network LAN environment of 100MB / 1GB switches with VLAN capability.
        ii. Operating system Microsoft Windows 10
        iii. Workstation systems use Windows 10
    b. Internet browser software to be configured per Manitoba's preference, within the requirements of Contractor ITSEC and (if required) PCI compliance. Chrome, Firefox
    c. Contractor will provide dual monitors on the agent workstation as available
    d. Contractor will provide at-home agents, if used on the program, with a webcam for video conferencing as available
    e. Contractor will provide internet access as required to interface with Manitoba applications
    f. Contractor will provide Jabra BIZ 1500 headsets (or an equivalent substitute) for voice agents
    g. Contractor and Manitoba agree that workstation monitor set up in the training environment may differ from the operations environment

SECTION III – STAFFING SOLUTIONS

1. **Recruiting and Hiring**
    a. Contractor will develop a customized agent profile(s) for recruiting and hiring purposes based on Manitoba's needs; each profile(s) will be developed with Contact Types in mind
    b. Contractor will ensure all candidates possess the approved combination of skill set and cultural alignment with the Manitoba based on the customized profile
    c. Contractor will deploy standard recruitment strategies to recruit agent candidates in accordance with local labor laws to meet all minimum requirements of the agent profile(s)
    d. Contractor will complete (or will have completed in the 12 month period prior to the Effective Date) Criminal Background Checks on all personnel providing Services which shall include at minimum a Canadian Criminal Background Check that includes the RCMP National Repository of Criminal Records.
        i. Due to COVID-19 related service interruptions, Contractor's responsibility to conduct background checks may in some cases be limited to due diligence of information reasonably available.
    e. Contractor will provide all personnel roster information to Manitoba three (3) Business Days prior to training. The Parties agree that the roster delivery date may be amended from time to time based on business needs (e.g. fast ramp).
    f. Subject to Section 3 of Schedule B of the Services Agreement, Contractor retains all final hiring or removal decisions on all personnel assigned to Manitoba

2. **Training**

    a. Manitoba will be responsible for building and maintaining all training materials for the Services
    b. Manitoba will set up all virtual training environments. The Parties will collaborate to ensure all trainees have access credentials in advance of their training start date.
    c. Contractor shall conduct orientation of their agents and train them on the relevant Contractor systems in advance of Services-specific training.
    d. Manitoba will conduct all Services-specific training of agents and leadership resources for the duration of the Services.
    e. Contractor shall ensure that a leader responsible for the attendance and performance of Agents is in attendance for all training classes.

f. New hire training for all required headcount will be billed at the agreed upon new hire training rate outlined in Section V - Cost Schedule
    i. If Manitoba makes a change to process or an update to the product offering that requires additional training, Contractor will bill for all process or update training at the production paid hour rate provided Contractor shall advise Manitoba in writing prior to incurring any additional costs that the requested change and/or update will result in additional costs.
g. Any ongoing training required by Manitoba will be billed back at the production paid hour rate set out in Section V - Cost Schedule.
h. For any net headcount growth, whether temporary or permanent, Contractor will provide new hire training at the training rate set out in Section V - Cost Schedule.
i. Notwithstanding the foregoing, Contractor will cover the cost of training for the replacement of agents due to promotion or attrition once in production.

3. **Staffing and Schedule Planning**

a. 18(1)(b) & 28(1)(b) [redacted]
b. Contractor shall have a minimum baseline team of 100 agents performing the Services no later than by Dec 15, 2020 or such other date mutually agreed to by the parties.
c. Contractor shall, unless otherwise requested by Manitoba, increase the size of the team to 300 agents, with the ability to scale up to 450 agents, as soon as reasonably possible.
d. Contractor shall be responsible to schedule Agents and Leaders as appropriate across the hours of operation to maximize efficiency and effectiveness of the Services.
e. All efforts to increase or decrease the size of the team shall be commercially reasonable efforts.

SECTION IV – OPERATIONAL DELIVERY

1. **Quality Assurance**

a. Contractor and Manitoba will collaboratively develop a quality scorecard for the purpose of quality management and calibrations that reflects the goals of the program's Key Performance Indicators
b. Contractor will monitor agent performance quality by listening to calls and evaluating transcripts of written interactions and case notes
c. Contractor will monitor a minimum of five (5) transactions for each agent monthly
d. Contractor and Manitoba will participate in bi-weekly calibration sessions, where both teams collaboratively score interaction samples to ensure alignment on overall quality metric and strategy.
e. Contractor will provide real time coaching and ongoing training to ensure maintenance of knowledge investment and follow through on actionable items

2. **Operational Resources**

a. Manitoba will have the following operational support model assigned for the go live date within 14 days of executed agreement; any change to the support model or ratios will be subject to a Change Order.
b. The amount of time a shared resource spends on the account will be determined based on the needs of the business work activity required as agreed to by both Contractor and Manitoba:

i. Implementation Manager - assigned; for Phase One Activation
ii. Agents - dedicated
    1. Tier 1 - front line agents; Contractor shall assume all headcount requests are for Tier 1 agents unless otherwise specified
    2.
iii. Team Leader - dedicated at 1:15 ratio and minimum 1 per shift; additional Team Leaders available on an as-needed basis
iv. Quality Analyst – dedicated at 1:50 ratio; additional available on an as-needed basis
v. Operations Manager – 1:90; additional available on an as-needed basis
vi. Director of Operations – 1:250
vii. Resource ratios may be adjusted upon mutual agreement between Manitoba and Contractor

3. Meetings and Communication

a. The Parties will meet with key stakeholders on the Manitoba team on a regular basis to review program performance and discuss new solution recommendations. Frequency and topics are defined flexibly as follows:
    i. A weekly operations call of approximately 1 hour in length, attended by Manitoba's Operations Manager. Additional attendees (e.g. Quality Analyst, Team Leader, Director of Operations) may be included based on meeting topics. Once per month, the weekly operations call will provide a monthly summary and review the staffing plan (HC/FTE requirements) for the month ahead.
    ii. A bi-weekly quality calibration call as further described in Section IV, 1, d

4. Location and Infrastructure

a. Location
    i. Contractor will deliver the Services from an at-home model within Canada
        1. Shared support resources may be located at another campus or at-home model within the Contractor network within Canada.
    ii. If an additional region is added to this Statement of Work, a Change Order will be developed and mutually agreed up prior to launch within any additional region
b. Infrastructure
    i. Contractor will provide and maintain sufficient facilities, hardware and materials for the scope of the Services, along with covering expectations on Manitoba growth within the Term
    ii. At-home workstations will adhere to Contractor's Telecommuting policies including:
        1. External Telecommuting Security Standards
        2. Telecommuting Policy
        3. Telecommuting Agreement

5. Change Order Process

a. All requested changes by Contractor or Manitoba that are outside of the scope of this SOW and attached documentation will be submitted as a Change Order in a mutually agreeable format.
b. Each Change Order will clearly state the implications to the project regarding deliverables, timelines and budget. No work identified on the Change Order will proceed without prior approval from Manitoba.

SECTION V – COST SCHEDULE

1. Minimum Billing Structure
    a. Contractor's pricing methodology was built based on a minimum monthly total of 16,000 billable hours (roughly equivalent to 100 Full Time Headcount) per month. Should the number of billable hours per month fall below this amount for more than two (2) consecutive months (excluding the initial month of Service) for any reason other than Contractor's failure to provide the personnel, Contractor and Manitoba agree to renegotiate the pricing to reflect the lower volume.

2. Invoicing Contact and Terms
    a. Contractor will invoice Manitoba on a monthly basis with payment terms as set forth in the Services Agreement, based on the following cost schedule outlined below. All invoices should be sent directly to the contact identified in the Services Agreement.

3. Fee Schedule

PHASE 1: CORE CONTACT TRACING TEAM				
Recurring Pricing (CAD):	**Language**	**Rate**	**Unit of Measure**	**Notes**
		Winnipeg / **Moncton**		
Tier 1	English	18(1)(b) & 28(1)(b)	Paid Hour	Contractor assumes all Agent time (inclusive of in-shift paid Breaks) spent working on Manitoba's behalf is billable. Manitoba will not be responsible for unpaid breaks or other paid time off such as vacation.
Tier 1	English/ French		Paid Hour	
PHASE 2: ADDITIONAL RESOURCES				
Recurring Pricing (CAD):		**Rate**	**Unit of Measure**	**Notes**
		Winnipeg		
Team Leader	N/A	18(1)(b) & 28(1)(b)	Paid Hour	For additional resources above and beyond the ratios outlined in Section V, 2. Headcount requirements for these roles shall be mutually agreed upon.
Quality Analyst	N/A		Paid Hour	
Operations Manager	N/A		Per Month	
Director of Operations	N/A		Per Month	
Additional Labor Related Fees				
Overtime Premium	N/A	18(1)(b) & 28(1)(b)	Paid Hour	30% premium on the Effective Hourly Rate. For clarity, no overtime shall be incurred unless pre-approved by the Manitoba in writing.

New Hire Training	N/A	18(1)(b) & 28(1)(b) [redacted]	Paid Hour	80% of the Effective Hourly Rate
ABAY / Up-Training	N/A		Paid Hour	100% of the Effective Hourly Rate
Consulting Fees		**Rate**	**Unit of Measure**	**Notes**
Implementation Fee	N/A	18(1)(b) & 28(1)(b) [redacted]	One Time	Covers the installation of the entire scope of work as described herein. Includes project management, standard reporting development, IT integration services, and campus development. Implementation Fee to be included in the first invoice.
IT Development	N/A		Hour	Applies for any IT development related to change management, ad hoc reporting, or additional programming that is not described herein; charges based on mutually agreed project scope.
Training Curriculum Design/Development	N/A		Hour	Applies for any training curriculum development related to amending/expanding the training agenda, modules, or activities; charges based on mutually agreed project scope.
Data Loss Prevention	N/A		Per user/per year	Covers licenses required through ForcePoint. Will be invoiced in arrears as the team size grows. E.g. if 100 HC are added in Month 1, Manitoba will be invoiced for 100 DLP licenses in Month 2. Net growth in team size will be billed in subsequent months.

Schedule A to Statement of Work
Service Levels & Key Performance Indicators

The Parties agree to mutually develop SLA and KPI expectations within 30 days of the launch of the program, or as time reasonably allows. Such SLA and KPIs shall be appended to this SOW via the Change Order process.

Exhibit 2 – Information Manager Agreement

See attached.

Exhibit 3 – Information Sharing Agreement

See attached.

Exhibit 4 - Personnel and Security Requirements

Personnel

1. The Contractor must, for all positions handling protected or restricted Manitoba data and information, perform criminal background checks, as approved by the Civil Service Commission, based on job position (role, responsibility, authority). Criminal background checks must include the RCMP National Repository of Criminal Records for all staff positions with access to protected or restricted Manitoba data and information.

2. The Contractor must have security procedures revoking access to physical location(s) and all system access privileges and/or data within 24 hours of termination of employment. This must include any subcontracting or sub-processor agreements or arrangements.

3. The Contractor must advise Manitoba when access privileges are revoked and had privileges granted by Manitoba or third parties on behalf of the Contractor

Relationships with Subcontractors and Sub-processors

1. The Contractor must disclose to Manitoba the use of all subcontractors and sub-processors in the provision of the Services, which must include details related to the capacity in which the subcontractor or sub-processor will be used.

2. Any changes to subcontracting or sub-processing arrangements must be made in writing and approved by Manitoba before applying them to the Services provided, in support of Manitoba's requirements.

3. The Contractor must document how Manitoba's requirements flow to all subcontractors and sub-processors and how requirements satisfaction will be determined and provide copies to Manitoba upon request.

4. The Contractor must document the Manitoba data and information which will be shared with and used by its subcontractors and sub-processors, including procedures for protecting Manitoba data and information, and provide to Manitoba upon request.

5. The Contractor must ensure that security risks associated with subcontractors and sub-processors are defined and monitored.

Security Policies, Procedures and Practices

1. The Contractor must exercise appropriate standards of due care with respect to securing Manitoba data and information, through the use of a comprehensive set of documented current policies demonstrating how its security policies, procedures and practices are periodically reviewed, updated, audited and enforced.

2. The Contractor must have procedures in place for the protection of "personal information" and" personal health information" as defined in Manitoba's *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA) and regulations, as may be amended from time to time, which are reviewed for compliance with the Services, as applicable.

Access Control

1. The Contractor must have access control policies in place, including for subcontractors and sub-processors to ensure that only authorized personnel who perform the Services

2. The Contractor must have processes in place for access requests, access reviews and access termination that are auditable.

3. The Contractor must use multi-factor authentication for all personnel

4. The Contractor must ensure that all users are uniquely identified at all times.

5. The Contractor must ensure that clear text passwords will not be transmitted across the network at any time.

Breaches of Security

1. The Contractor must notify Manitoba immediately, in writing, of any security breach or suspected security breach with the potential to impact Manitoba's security or the security of Manitoba data and information maintained by the Contractor.

2. The Contractor must identify what steps are being taken to prevent a recurrence and provide a root-cause analysis for breaches of security upon request.

Exhibit 2 - Information Manager Agreement

This is Exhibit 2 to an Agreement between the Government of Manitoba ("Client") and 24-7 Intouch, Inc. ("Organization") and dated the 24th day of November, 2020 (the "Agreement").

Capitalized terms not defined in this Exhibit have the meanings assigned to them in the Agreement.

WHEREAS:

A. When providing Services under the Agreement entered into by the Parties on April 13, 2020, and the Statement of Work order signed on November 24, 2020, for services including providing COVID-19 case investigations, contact tracing and daily contact and follow up services, the Organization is an "information manager" as defined under *The Freedom of Information and Protection of Privacy Act* and *The Personal Health Information Act of Manitoba* ("FIPPA" and "PHIA"), respectively.

B. Manitoba, as a "trustee" under PHIA, is authorized to collect and maintain Personal Health Information under PHIA for the purpose of the administration and management of various government programs and services.

C. Manitoba and the Organization acknowledge that certain information to be provided to the Organization pursuant to the Agreement is "Personal Health Information" under PHIA and that:

(a) Manitoba may disclose the Personal Health Information to the Organization in order to receive information management and information technology services and storage (subsection 25(1) of PHIA);

(b) the Organization may use Personal Health Information provided to it by Manitoba only for the purpose of providing information management and information technology services to Manitoba (subsection 25(2) of PHIA);

(c) Manitoba and the Organization must enter into this Information Manager Agreement, which provides for the protection of the Personal Health Information against such risks as unauthorized access, use, disclosure, alteration or destruction in accordance with the regulations under PHIA (subsection 25(3) of PHIA);

(d) the Organization must comply with:

(i) the same requirements concerning the protection, retention and destruction of Personal Health Information that Manitoba is required to comply with under PHIA; and

(ii) the duties imposed on the Organization in this Information Manager Agreement (subsection 25(4) of PHIA); and

(e) Personal Health Information that has been provided to the Organization under this Information Manager Agreement is deemed to be maintained by Manitoba for the purposes of PHIA (subsection 25(5) of PHIA)

E. Manitoba and the Organization acknowledge that certain information to be provided to the Organization pursuant to the Agreement is "Personal Information" under FIPPA and that:

(a) Manitoba may disclose the Personal Information to the Organization in order to receive information management and information technology services (subsection 44.1(1) of FIPPA);

(b) The Organization may use Personal Information provided to it by Manitoba only for the purpose of providing information management and information technology services to Manitoba (subsection 44.1(2) of FIPPA).

(c) Manitoba and the Organization must enter into this Information Manager Agreement, which provides for the protection of the Personal Information against such risks as unauthorized access, use, disclosure, alteration or destruction in accordance with the regulations under FIPPA (subsection 44.1(3) of FIPPA);

(d) The Organization must comply with:

(i) the same requirements concerning the protection of Personal Information that Manitoba is required to comply with under FIPPA; and

(ii) the duties imposed on the Organization in this Information Manager Agreement (subsection 44.1(4) of FIPPA); and

(e) Personal Information that has been provided to the Organization under this Information Manager Agreement is deemed to be in the custody and control of Manitoba for the purposes of FIPPA (subsection 44.1(5) of FIPPA).

IN CONSIDERATION OF THE PARTIES ENTERING INTO THE AGREEMENT THE ORGANIZATION AND MANITOBA AGREE AS FOLLOWS:

SECTION 1.00 - DEFINITIONS, INTERPRETATION AND SCHEDULES

1.01 In this Information Manager Agreement, the following definitions shall apply:

(a) "**Agreement**" means the Agreement between the Parties as identified above;

(b) "**Personal Health Information**" has the meaning given to that term in *The Personal Health Information Act*, as amended from time to time, and is set out in Schedule "A" – Privacy Definitions;

(c) "**Personal Information**" has the meaning given to that term in *The Freedom of Information and Protection of Privacy Act*, as amended from time to time, and is set out in Schedule "A" – Privacy Definitions";

(d) "**Privacy Compliance Officer**" means the individual appointed by the Organization who shall have the responsibilities set out in subsections 8.03 and 8.04 of this Information Manager Agreement;

(e) "**Representatives**" has the meaning given to that term in the Agreement;

(f) "**Organization**" means 24-7 Intouch, Inc;

(g) "**Services**" means the services described in Schedule C-2 of the Agreement;

(h) "***The Freedom of Information and Protection of Privacy Act***" or "**FIPPA**" means *The Freedom of Information and Protection of Privacy Act* of Manitoba, C.C.S.M. c. F175, and the regulations under that Act, as amended from time to time;

(i) "***The Personal Health Information Act***" or "**PHIA**" means *The Personal Health Information Act,* C.C.S.M. c. P33.5, and the regulations under that Act, as amended from time to time; and

(j) "**Third Party**" means any person, corporation, organization or entity other than Manitoba or the Organization.

1.02 The requirements and obligations in this Information Manager Agreement respecting Personal Information and/or Personal Health Information:

(a) apply to all Personal Information and/or Personal Health Information provided to or acquired by the Organization, in any form, medium or manner, in the course of, or incidental to, the performance of the Agreement;

(b) apply whether such Personal Information and/or Personal Health Information was provided or acquired before or after the commencement of the Agreement; and

(c) continue to apply after the termination or expiration of the Agreement.

1.03 The following Schedules form part of this Information Manager Agreement:

(a) Schedule "A" – Privacy Definitions;

(b) Schedule "B" – Electronic Media Disposal Standards and Procedures;

(c) Schedule "C" – Certificate of Destruction of Information;

(d) Schedule "D" – Pledge of Confidentiality.

SECTION 2.00 - TERM OF AGREEMENT

2.01 This Information Manager Agreement comes into effect on the Effective Date of the Agreement and shall continue to apply until all the obligations of the Organization under this Information Manager Agreement are completed.

SECTION 3.00 - PURPOSE OF THIS AGREEMENT

3.01 The purpose of this Information Manager Agreement is to set out the obligations of the Organization, as the Information Manager, respecting the protection of Personal Information and/or Personal Health Information against such risks as unauthorized access, use, disclosure, alteration, storage or destruction, in accordance with the requirements set out in subsection 44.1(3) of FIPPA and subsection 25(3) of PHIA and the regulations under those Acts.

SECTION 4.00 - REPRESENTATIONS AND WARRANTIES

4.01 The Organization represents and warrants that:

(a) the Organization is aware of and understands Manitoba's responsibilities as a "trustee"

of Personal Health Information under PHIA and the Organization's own responsibilities as an "information manager" under FIPPA and PHIA, and will be able to meet those responsibilities; and

(b) the Organization understands Manitoba's requirements respecting the protection of Personal Information and/or Personal Health Information under the Agreement, and this Information Manager Agreement, and will satisfy these requirements.

SECTION 5.00 - OWNERSHIP AND PROTECTION OF INFORMATION

5.01 The Organization acknowledges and agrees that, for the purposes of FIPPA, PHIA and the Agreement, Manitoba is the exclusive owner and has custody and control of all Personal Information and maintains all Personal Health Information provided to or acquired by the Organization under the Agreement.

5.02 Nothing in the Agreement confers on the Organization any title to or right or interest in any Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement.

5.03 While Personal Information and/or Personal Health Information is in the possession of the Organization, the Organization shall take all reasonable precautions to protect it from:

(a) such risks as unauthorized use, access, disclosure, alteration, storage, retention and destruction; and

(b) fire, theft, vandalism, deterioration, accidental destruction, loss and other administrative, operational and physical security hazards.

SECTION 6.00 – STORAGE, RETURN AND DESTRUCTION OF INFORMATION

6.01 The Organization shall not store, access or use any Personal Information and/or Personal Health Information on its computers or equipment, including remote access from the Organization's office and server locations, outside Canada, except with the express written consent of Manitoba.

6.02 The Organization shall return, transfer or destroy Personal Information and/or Personal Health Information as the directed by Manitoba:

(a) upon completion of the Organization's obligations under the Agreement;

(b) on expiration of the Agreement;

(c) on termination of the Agreement for any reason; or

(d) on request of Manitoba,

and the Organization shall not keep or maintain any copies, in any form or medium, of any Personal Information and/or Personal Health Information.

6.03 The return of Personal Information and/or Personal Health Information prescribed by subsection 6.02 shall be carried out immediately in a safe and secure manner, as directed by Manitoba, acting reasonably, in the form or format in which such information exists at the time of expiration,

termination or request.

6.04 Where the Organization is directed by Manitoba or required by this Information Manager Agreement to destroy Personal Information or Personal Health Information, or a copy of Personal Information or Personal Health Information, the Personal Information and/or Personal Health Information shall be destroyed in a manner which:

(a) adequately protects the confidentiality of the Personal Information or Personal Health Information;

(b) is appropriate to the medium in which the Personal Information and/or Personal Health Information is recorded; and

(c) is in accordance with the standards for the disposal of information as set out in the Electronic Media Disposal Standards and Procedures attached to this Information Manager Agreement as Schedule "B".

6.05 The Organization shall provide written confirmation of destruction to the Manitoba Contract Manager, in the form of the Certificate of Destruction of Information attached to this Information Manager Agreement as Schedule "C".

SECTION 7.00 - GENERAL CONFIDENTIALITY PROVISIONS

7.01 While the Agreement is in effect, and at all times thereafter, the Organization and the officers, employees and agents of the Organization:

(a) shall treat as strictly confidential all Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement;

(b) shall not:

(i) use, modify, view, aggregate or destroy Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement except for the proper performance of the Organization's obligations under the Agreement, or

(ii) disclose Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement to any Third Party, except in accordance with this Information Manager Agreement, and

(iii) retain or store any record containing Personal Information and/or Personal Health Information, or create or compile a record containing Personal Information and/or Personal Health Information, except for the client list disclosed by Manitoba to the Organization through a file transfer protocol site (i.e., Axway) or as agreed upon by the Parties.

(c) shall:

(i) take all reasonable steps to ensure that no person views, uses or discloses Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement except for the proper performance of the Organization's obligations under the Agreement or in accordance with this Information Manager Agreement; and

(ii) comply with any reasonable rules or directions made or given by Manitoba with respect to safeguarding or ensuring the confidentiality of Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement.

SECTION 8.00 - GENERAL PRIVACY COMPLIANCE REQUIREMENTS

8.01 The Organization shall comply with the same requirements concerning the protection, retention and destruction of Personal Health Information that Manitoba is required to comply with as a "trustee" under PHIA.

8.02 The Organization shall comply with the same requirements concerning the protection, retention and destruction of Personal Information that Manitoba is required to comply with under FIPPA.

8.03 The Organization, through its Privacy Compliance Officer (referred to in subsection 8.04), shall ensure that all its Representatives who have or may have access to Personal Information and/or Personal Health Information are aware of the requirements, obligations and procedures respecting the collection, use, protection, retention, disclosure, alteration and destruction of Personal Information and/or Personal Health Information, including specifically, Personal Information and/or Personal Health Information in FIPPA, PHIA, the regulations under those Acts, the Agreement, including this Information Manager Agreement, and shall take all reasonable steps to ensure that all Representatives comply with these requirements, obligations and procedures.

8.04 The Organization shall appoint an officer or employee of the Organization as its Privacy Compliance Officer, whose responsibilities shall, in addition to those described in subsection 8.03, include:

(a) ensuring that all Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement is securely maintained and protected while at the data centres, in accordance with section 11.00 of this Information Manager Agreement and Exhibit 4 to the Agreement (Personnel and Security Requirements); and

(b) monitoring and ensuring compliance by the Organization with FIPPA, PHIA, the regulations under those Acts and the Agreement, including this Information Manager Agreement.

8.05 The Organization shall ensure that each of its Representatives who has access to Personal Information or Personal Health Information:

(a) signs a Pledge of Confidentiality, in the form attached as Schedule "D";

(b) is made fully aware of the consequences of breaching the requirements and obligations in the Agreement, including this Information Manager Agreement, or of breaching the Organization's security policies and procedures under section 11.00; and

(c) is subject to a criminal records check in accordance with section 5.14 of Schedule B of the Agreement and the Service Schedules.

SECTION 9.00 - AUTHORIZED USE OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

9.01 The Organization shall only use Personal Information and/or Personal Health Information, and shall ensure that its Representatives only use the Personal Information and/or Personal Health

Information, for the purposes of performing the Organization's obligations under the Agreement and providing the Services in accordance with the Agreement, and for no other purpose, including to aggregate or data mine Personal Information and/or Personal Health Information.

9.02 The Organization shall:

(a) limit use of and access to Personal Information and/or Personal Health Information to those Representatives who:

(i) have first signed a Pledge of Confidentiality in the form attached as Schedule "D";

(ii) need to know the Personal Information and/or Personal Health Information for the purpose of carrying out the Organization's obligations under the Agreement and providing the Services; and

(iii) are designated by the Organization in writing as being authorized to use and access the Personal Information and/or Personal Health Information. The Organization shall provide a list of the name and position of each authorized Representative prior to the commencement of Services by the Organization. The Organization shall not make any changes to these designated Representatives without providing prior written notice of the changes to Manitoba.

(b) for each of its Representatives who is authorized to have access to the System or any Personal Information and/or Personal Health Information, determine the Personal Information and/or Personal Health Information that he or she is authorized to access;

(c) limit all access to and every use of Personal Information and/or Personal Health Information by the authorized Representatives to the minimum amount necessary to perform the Organization's obligations under the Agreement and to provide the Services in accordance with the Agreement; and

(d) ensure that all its Representatives who have or may have access to Personal Information and/or Personal Health Information, including specifically Personal Information or Personal Health Information are aware of the requirements, obligations and procedures respecting the collection, use, protection, retention, disclosure, alteration, storage and destruction of Personal Information and/or Personal Health Information in FIPPA, PHIA, the regulations under those Acts, and the requirements in the Agreement, including this Information Manager Agreement, for the purpose of understanding their undertakings in the Pledge of Confidentiality.

9.03 If during the Term of the Agreement, the Organization becomes aware that any designated Representative has a criminal record, the Organization shall promptly notify Manitoba and writing and, unless otherwise agreed to by Manitoba in writing, not permitted such designated Representative to access Personal Information and/or Personal Health Information. .

9.04 The Organization shall take all reasonable steps to ensure that:

(a) no person removes any Personal Information and/or Personal Health Information, or any copy of Personal Information and/or Personal Health Information, in any form or medium, from the Organization's premises or information technology systems from which or through which the Services are carried out;

(b) no person retains or makes unauthorized copies of Personal Information or Personal

Health Information, in any form or medium;

(c) no person discloses any Personal Information or Personal Health Information, except as specifically authorized under section 10.00; and

(d) no person modifies or alters any Personal Information or Personal Health Information, in any manner that is not specifically authorized under the Agreement.

9.05 The Organization and its Representatives:

(a) shall not use any Personal Information and/or Personal Health Information to contact, directly or indirectly, any individual for any purpose except to the extent necessary to properly provide the Services hereunder;

(b) shall not use Personal Information and/or Personal Health Information to develop, establish, expand, modify or maintain a database or other collection of information in any form or medium except to the extent necessary to properly provide the Services and carry out the obligations of the Organization under the Agreement; and

(c) shall not link or match with any other information, except to the extent necessary to properly provide the Services and carry out the obligations of the Organization under the Agreement.

9.06 The Organization shall take all reasonable steps to ensure that no person other than Manitoba uses, links or matches Personal Information and/or Personal Health Information provided to or acquired by the Organization under the Agreement except to the extent necessary to properly provide the Services and carry out the obligations of the Organization under the Agreement.

SECTION 10.00 - RESTRICTIONS RESPECTING DISCLOSURE OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

10.01 The Organization shall not give access to or disclose, and shall take all reasonable steps to ensure that no person gives access to or discloses Personal Information and/or Personal Health Information to any Third Party except as follows:

(a) to Representatives of the Organization who are authorized to use and have access to the Personal Information and/or Personal Health Information under paragraph 9.02(a)(iii) of this Information Manager Agreement, to the extent those Representatives need to know the information for the purposes of performing the Organization's obligations in this Information Manager Agreement and providing the Services in accordance with the Agreement;

(b) for the purposes of providing Services in accordance with the Agreement;

(c) where disclosure is required by the laws of Canada or Manitoba; and

(d) where disclosure is required by an order of a court, person or body with jurisdiction to compel production of the Personal Information and/or Personal Health Information or is required to comply with a rule of court that relates to the production of the Personal Information or Personal Health Information.

10.02 Without limiting subsection 10.01 of this Information Manager Agreement, the Organization shall not:

(a) sell or disclose any Personal Information or Personal Health Information, for consideration; or

(b) exchange any Personal Information and/or Personal Health Information for any goods, services or benefit; or

(c) give any Personal Information and/or Personal Health Information to any Third Party for any purpose, including (but not limited to) solicitation for charitable or other purposes, except as permitted under subsection 10.01; and shall take all reasonable steps to ensure that none of these activities take place.

SECTION 11.00 - PROTECTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION AND SECURITY ARRANGEMENTS

11.01 The Organization shall put in place security safeguards, including administrative, operational and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the Personal Information and/or Personal Health Information, and protect the Personal Information and/or Personal Health Information against such risks as unauthorized use, access, disclosure, alteration, retention or destruction. These security safeguards shall take into account the sensitivity of the Personal Information and/or Personal Health Information and the medium in which the information is stored, handled, transmitted or transferred. Upon request Manitoba shall review any safeguard established by the Organization and provide its approval or requested amendments regarding same.

11.02 Without limiting subsection 11.01 of this Information Manager Agreement, the Organization shall use Commercially Reasonable Efforts to comply with the security safeguards prescribed in Exhibit 4 to the Agreement (Personnel and Security Requirements).

11.03 The Organization must conduct an audit of its security safeguards at least once every two years after the commencement of Services by the Organization in accordance with the requirements of FIPPA, PHIA and the regulations under those Acts.

11.04 If an audit referred to in subsection 11.03 identifies deficiencies in the Organization's security safeguards, the Organization shall, as soon as practicable:

(a) prepare a plan for correcting the deficiency and provide that plan to Manitoba; and

(b) provide Manitoba with reports on the correction being made; and

(c) such other measures as are identified in Exhibit 4 to the Agreement (Personnel and Security Requirements).

11.05 The Organization shall establish, or have established, written policies and procedures respecting the use of, access to, disclosure, storage, protection, security and destruction of the Personal Information and/or Personal Health Information, which shall be consistent with and reflect the requirements of the Agreement, including this Information Manager Agreement. Upon request, Manitoba shall review any policies or procedures established by the Organization and provide its approval or requested amendments regarding same.

11.06 The written policies and procedures shall include:

(a) measures to ensure the security of Personal Information and/or Personal Health

Information when a record of the information is removed from a secure designated area;

(b) measures to ensure the security of Personal Information and/or Personal Health Information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;

(c) provisions for the recording of security breaches;

(d) corrective procedures to address security breaches; and.

such other measures as are identified in Exhibit 4 to Agreement (Personnel and Security Requirements)

11.07 The written policies and procedures put into place by the Organization respecting Personal Health Information and Personal Information shall be consistent with and reflect the requirements of PHIA and FIPPA, including the safeguards for electronic health information systems prescribed in section 4 of the *Personal Health Information Regulation* (Man. Reg. 245/97).

11.08 The Organization shall regularly review the Organization's record user activities respecting Personal Information and/or Personal Health Information, including specifically Personal Health Information and Personal Information to detect any security breaches.

11.09 The Organization shall comply with the written policies and procedures respecting the use of, access to, disclosure, storage, protection, security and destruction of Personal Information and/or Personal Health Information.

11.10 Manitoba shall provide baseline training documentation and materials to Organization as soon as reasonably possible covering the requirements of FIPPA, PHIA, and the Agreement, as contemplated in the Agreement. The Organization may add to these materials and will provide orientation and ongoing training for its Representatives about the requirements of FIPPA, PHIA and the Agreement, including this Information Manager Agreement, respecting the protection of Personal Information and/or Personal Health Information and about the Organization's written policies and procedures.

11.11 In addition to complying with the requirements and obligations in this Information Manager Agreement, the Organization shall comply with any additional, reasonable requirements established by Manitoba from time to time to protect the Personal Information and/or Personal Health Information. If any such additional requirements result in additional costs to the Organization, Manitoba will reimburse the Organization for those additional costs to the extent that they are specific to Manitoba.

SECTION 12.00 - RECORDS OF ACCESS TO AND USE AND DISCLOSURE PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

12.01 While the Agreement is in effect, the Organization shall maintain the following records:

(a) records respecting all use of and access to Personal Information and/or Personal Health Information by the Organization and its Representatives;

(b) copies of all Pledges of Confidentiality required under clause 8.05(a) of this Information Manager Agreement;

(c) copies of all designations of authorized Representatives and of all determinations respecting the Personal Information and/or Personal Health Information required under

paragraph 9.02(a)(iii) and clause 9.02(b) of this Information Manager Agreement;

(d) records of all disclosures of Personal Information and/or Personal Health Information;

(e) records of the Organization's security policies and procedures respecting Personal Information and/or Personal Health Information including specifically Personal Information and/or Personal Health Information; and

(f) records of all security breaches and corrective procedures put in place, as required under clauses 11.06(c) and (d) of this Information Manager Agreement.

SECTION 13.00 - REPORTS TO MANITOBA RESPECTING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

13.01 The Organization shall, immediately upon becoming aware of any of the following, notify Manitoba in writing of:

(a) any unauthorized use of, access to, disclosure, alteration, retention or destruction of Personal Information or Personal Health Information; and

(b) any breach (actual or threatened) of any term or condition of the Agreement with full details of the unauthorized use, access, disclosure, alteration, retention or destruction or of the breach. The Organization shall immediately take all reasonable steps to prevent the recurrence of any unauthorized use, access, disclosure, alteration, retention or destruction of Personal Information or Personal Health Information, or to remedy the breach, and shall promptly, and in writing, notify Manitoba of the steps taken.

SECTION 14.00 - INSPECTIONS, REVIEWS AND AUDITS RESPECTING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

14.01 When requested by Manitoba, the Organization agrees to carry out a review of the Organization's information practices as they relate to the Organization's access to, use, disclosure, storage, protection, security and destruction of Personal Information and/or Personal Health Information pursuant to the Agreement. The Organization shall provide copies of the results of any review to Manitoba within twenty-four (24) hours of completing the review.

14.02 Manitoba or its agents shall be entitled, at any time, to inspect and audit the operations of the Organization, including the premises where any of the Services are provided to monitor access to and use of any Personal Information or Personal Health Information.

14.03 Manitoba shall provide the Organization with ten (10) days written notice prior to conducting its inspections and audits. The Organization shall cooperate with Manitoba when it is conducting such inspections and audits.

14.04 If any inspection, review or audit identifies deficiencies in the Organization's information practices, the Organization shall take steps to correct the deficiencies immediately and shall promptly notify Manitoba in writing as to the steps taken.

SECTION 15.00 - MATERIAL SERVICE FAILURE

15.01 For the purposes of subsection 1.7(d)(ii) of the SoW, but subject to subsection 15.02 below, Manitoba shall be entitled to declare that a Material Service Failure has occurred where Manitoba

is reasonably of the opinion that the Organization:

(a) has used, permitted access to or disclosed, altered or retained Personal Information and/or Personal Health Information, including Personal Information or Personal Health Information, in a manner which is not authorized under the Agreement, including this Information Manager Agreement, or is about to do so; or

(b) has not adequately protected Personal Information and/or Personal Health Information, including Personal Information or Personal Health Information, from the risks identified in clauses 5.03(a) and (b); or

(c) has made a false or misleading warranty or representation; or

(d) has failed to comply with, or is about to fail to comply with, any of its obligations or undertakings under this Information Manager Agreement.

15.02 In the event Manitoba has declared that a Material Service Failure has occurred in accordance with subsection 15.01 above, then Manitoba shall have the right to immediately terminate the Agreement.

15.03 On termination of the Agreement for any reason, the Organization shall, unless otherwise agreed to by Manitoba and the Organization in writing, immediately refrain from any further use of, access to, disclosure of or transactions involving any Personal Information and/or Personal Health Information and the Organization shall, as directed by Manitoba, immediately:

(a) return all Personal Information and/or Personal Health Information provided to the Organization under the Agreement in accordance with subsection 6.03 of this Information Manager Agreement; and

(b) as and when directed by Manitoba, and in any event no later than 14 from the date when the Organization ceases to perform any further Services for Manitoba, ensure any other copies of Personal Information and/or Personal Health Information and other information provided to the Organization under the Agreement, in any form or medium, are destroyed in a manner that adequately protects the confidentiality of the Personal Information and/or Personal Health Information as required under subsection 6.03 of this Information Manager Agreement. The Organization shall provide written certificate of destruction to Manitoba the form of the Certificate of Destruction of Information attached to this Information Manager Agreement as Schedule "C".

15.04 Those sections that by their very nature are intended to survive the termination or expiration of this Agreement shall survive the expiration or termination of this Agreement.

15.05 This Agreement may be executed in counterparts delivered by facsimile transmission or electronic communication producing a printed copy, each of which shall be deemed to be an original, and all of which shall be considered one and the same instrument.

This Information Manager Agreement has been executed on behalf of the Organization and on behalf of Manitoba, by its duly authorized representatives, on the dates noted below.

26 [redacted]

SIGNED IN THE PRESENCE OF:

17(1) & 17(3)(e)

Witness

FOR THE GOVERNMENT OF MANITOBA

17(1) & 17(3)(e) or designate)

Name: Katch Herd

Position: Deputy Minister

Date: NOV 2 4 2020

17(1) & 17(3)(e)

Witness

FOR 24-7 INTOUCH, INC.

17(1) & 17(3)(e)

Name: Mitul Kotecha

Position: President

Date: Nov-24-2020

This is Schedule "A" to the Information Manager Agreement between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

PRIVACY DEFINITIONS

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT:

"personal information" means recorded information about an identifiable individual, including

(a) the individual's name,

(b) the individual's home address, or home telephone, facsimile or e-mail number,

(c) information about the individual's age, sex, sexual orientation, marital or family status,

(d) information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,

(e) information about the individual's religion or creed, or religious belief, association or activity,

(f) personal health information about the individual,

(g) the individual's blood type, fingerprints or other hereditary characteristics,

(h) information about the individual's political belief, association or activity,

(i) information about the individual's education, employment or occupation, or educational, employment or occupational history,

(j) information about the individual's source of income or financial circumstances, activities or history,

(k) information about the individual's criminal history, including regulatory offences,

(l) the individual's own personal views or opinions, except if they are about another person,

(m) the views or opinions expressed about the individual by another person, and

(n) an identifying number, symbol or other particular assigned to the individual;

THE PERSONAL HEALTH INFORMATION ACT:

"personal health information" means recorded information about an identifiable individual that relates to

(a) the individual's health, or health care history, including genetic information about the individual,

(b) the provision of health care to the individual, or

(c) payment for health care provided to the individual,

and includes

(d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and

(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;

26 [redacted]

This is Schedule "B" to the Information Manager Agreement between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

See attached.

Business Transformation and Technology

Manitoba Government

Electronic Media Disposal Standards and Procedures

Version 1.0 November 2005

Manitoba

Table of Contents

Introduction

Background

This document provides standards and procedures for the secure reuse and disposal of computer media containing government information. The Information Protection Centre (IPC) developed and maintains this document under the direction of Manitoba Information and Communications Technologies. The standards and procedures are necessary to ensure that confidential government information, personal, personal health, or other identifying information about third parties or businesses, cannot be retrieved from computer media accidentally or intentionally, by unauthorized persons within or outside of the Manitoba government.

This document includes standards and procedures for a number of media types. Various media types can have a significantly different standard and procedure for the safe removal of data.

Government Records

Retention and disposal of government records is governed by *The Archives and Recordkeeping Act* (ARA). Most e-mail messages, documents and other electronic records created or received in the course of government business are **government records**. This means that the records must be captured (filed) in a recordkeeping system, and retained and disposed of according to the provisions of an approved records schedule.

Government employees are responsible for ensuring that government records under their control are properly retained and disposed of.

Prior to destroying information or disposing of media containing government information, it is critical that the user (or the employee or work group responsible for the information) ensure that all information and records required for government business and recordkeeping purposes have been retained and managed in accordance with the ARA.

Employees must follow proper procedures for managing and disposing of electronic documents created or received in the desktop environment, including e-mail and other files created using desktop applications and stored in network servers, computer hard drives or removable storage media.

Government records maintained in electronic form in other types of systems are subject to the same requirements for authorized retention and disposal. This means that retention rules should be defined in advance and reflected in approved records schedules, and that provision must be made to ensure the records are maintained, protected, and accessible for as long as required – whether in native formats in the original system, or in other appropriate formats, systems or media. Responsibility for defining the retention requirements and preparing records schedules rests with the business area responsible for the records. IT specialists must ensure that all data required to support, manage and access these electronic records is retained, prior to disposing of data on computer storage media.

Disposal Standard for Hard Disk Drives

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of hard drive assets including disposal.

Hard drive assets that are to be reused elsewhere within government departments must be wiped to ensure all data is unavailable for inappropriate access.

Hard drive assets that are being disposed outside of government must be wiped or destroyed to ensure all data is unavailable for inappropriate access.

The destruction of information or disposition of hard drives containing government information must be managed in accordance with *The Archives and Recordkeeping Act.*

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE function that does not result in the secure deletion of the data stored on the hard drive; rather file and directory pointers are erased without ever touching the actual data. As a result of this process, data that is erased using the operating system DELETE/ERASE function can be easily recovered.

Many devices including, but not limited to, printers, photocopiers, and multifunction devices include hard drives. The hard drives in these devices can retain sensitive information that can be easily recovered.

Hard drives used by the Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the hard drive disposal standard and procedure.

Standard

As a general principle, all private, valuable, and confidential data should be stored on Network file servers where proper backup and recovery procedures are in place. Local workstation hard drives are not backed up as part of standard operating procedures. The following paragraphs outline the steps required to dispose of a hard drive depending on the specific circumstance.

Transfer of hard drives within a department: Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. If the hard drive is remaining within the department, the drive can be reformatted prior to transfer because special recovery tools would be required by an individual to access the data erased on the hard drive. In the event the hard drive contained sensitive information it is recommended that it be sanitized using the disk wiping procedures outlined in the procedure section of this document unless the hard drive has been encrypted using Government approved encryption software.

Disposal of hard drives to other departments or organizations outside of the Government: Prior to disposal or transfer to another department, working, usable hard drives must be overwritten in accordance with the disk wiping procedures. The owner must be able to certify that the hard drive was properly sanitized. Certification should include the make, model, and government asset tag number of the computer or stand alone hard drive and the date that the procedure was performed. Equipment designated for surplus or other disposal must have some form of identification stating that the hard drive has been properly sanitized. This could include a physical label or some form of electronic identification written to the hard drive.

Repairing a hard drive under warranty:

Hard drive manufactures and computer suppliers typically require the return of defective hard drives under warranty. Some suppliers will allow customers to declare when certain hard drives contain sensitive information by completing the required declaration forms. Drives that have been verified by the manufacturer as defective do not have to be returned to the manufacturer. The failed hard drive must then be destroyed following the procedures for hard drive disposal.

When the manufacturer requires that the failed disk drive be returned for warranty, and the hard drive is unencrypted, a risk assessment must be conducted to determine the sensitivity of the data on the hard drive. If there is potentially sensitive data on the failed hard drive then the old drive must be properly destroyed and the owner of the system must assume any costs associated with purchasing a new drive.

Hard drives can be returned for warranty repair or replacement without concern for the sensitivity of the data when the hard drive is encrypted or part of a file server configured with RAID 5 (Redundant Array of Inexpensive Disks), and the data spread across three or more disks.

Disposal of damaged or inoperable hard drives off warranty: For hard drives that are off warranty and inoperable the drives must be physically destroyed.

Return of leased equipment: Lease agreements typically require that equipment be returned intact to the leasing company. Workstation hard drives must have the data sanitized using the

disk wiping procedures. Certain devices have hard drives but cannot run the disk wiping software, including but not limited to, certain proprietary servers, printers, fax machines, or other multi function devices. For these types of devices the hard drives must be destroyed or degaussed and the owner of the device must assume any associated costs. When negotiating lease arrangements considerations must take into account the requirements of this standard.

Roles and Responsibilities

End users are responsible for erasing all personal and business data from their hard drives before return to the department.

Departments are responsible for ensuring that all hard drives are wiped before they are made available for new use within Government.

Departments are responsible for ensuring that all surplus hard drives are disposed of in accordance with the disposal standard.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

MICT is responsible for ensuring that all surplus computer equipment destined for Computers for Schools and Libraries are wiped of all sensitive information.

There must be an audit trail that shows hard drives have been wiped, degaussed, or physically destroyed at the appropriate time.

Procedure - Disposal of Hard Drives

Methods for Secure Information Disposal

There are three primary methods for secure disposal of hard drives. Total destruction and disk wiping are the two preferred methods. Hard disk degaussing is not recommended due to the high cost of hard disk degaussing equipment and the complexity of the degauss process. If degaussing equipment and trained staff are available then degaussing is an acceptable method of erasing data.

1) Total Destruction

The Manitoba Government donates surplus computer equipment to Computers for Schools and Libraries. Therefore total disk destruction is not the preferred method of disposal for hard drives in personal desktop or laptop computers.

For file servers it must decided whether the extra cost and time involved in wiping is justified. Disk erasure software is often incompatible with proprietary server hardware. Departments should consider whether the cost associated with the secure disposal will exceed the value of the asset. If it is more cost effective, then choose total destruction by an approved vendor as the primary option for server hard drives.

2) Disk Wiping (Overwriting)

Disk wiping software involves methods of writing 1's to the entire disk, followed by writing 0's on top of the previous 1's. With each pass the chance of recovery is greatly reduced. A minimum of 1 pass is required with 3 passes required for highly confidential or extremely sensitive information. Government hard disks sent to Computer for Schools and Libraries must be wiped once at source (originating location) and a second time at Computers for Schools and Libraries using Government approved disk wiping software.

3) Degaussing

Degaussing magnetically erases data from magnetic hard drives. When done properly, it renders any previous stored data unreadable. Degaussing requires the purchase of a degaussing product, frequent product testing and a skilled operator. The result of degaussing can vary depending on how it is performed. Hard disk degaussing renders the hard drive inoperable. For this reason degaussing is not recommended for drives that will be sent to Computers for Schools and Libraries. Hard disk degaussing is also not recommended because of the high costs associated procuring degaussing equipment. When degaussing equipment and skilled operation staff are available degaussing is an acceptable alternative for drives that are not going to Computers for Schools and Libraries and for hard drives that have failed or are from proprietary servers that cannot run the disk wiping software.

Disposal Standard for Magnetic Tapes

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of magnetic tapes.

All magnetic tapes that have not been degaussed must be physically destroyed when disposing of the magnetic tape media.

To prevent loss of privacy, magnetic tapes that are to be reused elsewhere within government must be carefully degaussed to remove proprietary government information.

The destruction of information or disposition of magnetic tapes containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Magnetic tape media used by the Government of Manitoba may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this material must be the primary goal of the magnetic tape disposal process.

Standard

As a basic principle, magnetic tapes must be securely degaussed each time they are used in a new application environment. For example a magnetic tape used to backup a sensitive production system must be securely degaussed before reuse within the application environment for backing up a less sensitive information system. This ensures that no residual data from the sensitive production system remains on the magnetic tape.

Degaussing of magnetic tape must be performed with a degaussing unit of sufficient field strength for the media being sanitized. Refer to the manufacturer specification for the magnetic tape degaussing unit.

Magnetic tapes must not be reused in other departments, boards, agencies, or special operating agencies without degaussing.

Magnetic tapes that have not been degaussed, and are no longer of use to back-up or store information, must be securely physically destroyed.

Roles and Responsibilities

Departments are responsible for degaussing or physically destroying of all magnetic tapes.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that magnetic tapes have been disposed of in an appropriate fashion through either degaussing or physical destruction. There must be an audit trail that shows all magnetic tape has been degaussed or physically destroyed at the appropriate time.

Procedure - Disposal of Magnetic Tape

As a minimum precaution magnetic tapes must be degaussed:

- When returned for warranty replacement
- When leaving the Government's controlled environment
- Prior to reuse in a new application environment
- Prior to reuse in other Government Departments, or
- When going to disposal without physical destruction.

In environments where no degaussing equipment exists, or when the tapes contained highly sensitive information, the magnetic tapes must be physically destroyed prior to disposal. Shredding is the preferred method for destroying magnetic tape media.

Commercial shredding operations offer mobile shredding services. Tapes destroyed using mobile shredding services do not require degaussing prior to destruction provided the shredding operation is monitored and validated by Government staff.

Physical destruction of media via incineration is typically not recommended. Although this may be effective physical destruction method safety, environmental and/or health concerns preclude using such procedures.

Disposal Standard for Optical (CD/DVD) Media

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of optical media. For the purpose of this document optical media includes, but is not limited to, read only and rewriteable compact disks (CD) and digital video/versatile disks (DVD).

Optical media has no secure erase capability; as a result, secure disposal, destruction, is the only viable option for this media type.

The destruction of information or disposition of optical media containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Optical media used by the Government of Manitoba may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the optical media disposal standard and procedure.

Standard

When the optical media is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed.

When optical media is used to dispense licensed software, physical destruction of the media should occur in conjunction with the expiration of the software license.

If the media content is particularly sensitive, shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical.

Roles and Responsibilities

Departments are responsible for physical destruction of all optical media.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that optical media has been disposed of in an appropriate fashion. There must be an audit trail that shows all optical media has been physically destroyed at the appropriate time.

Procedure - Disposal of Optical Media

When the CD or DVD storage media is no longer of use it must be physically destroyed.

Methods for Secure Information Disposal

Shredding is the preferred disposal method for optical media.

Multiple shredding passes are not normally recommended as this can create excessive plastic dust which is not appropriate in an office environment.

Physical destruction of media via sanding, or incineration, is typically not recommended. Although these may be effective physical destruction methods, safety, environmental and/or health concerns preclude using such procedures.

Government departments should consider the use of commercial shredding operations to safely destroy their optical storage media when appropriate shredding equipment is not available within the department.

Disposal Standard for Diskettes

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of diskettes including disposal. For the purpose of this document the term diskette refers to soft, or flexible, media types such as floppies and Zip disks and does not include CD or DVD media.

Before disposal all Diskettes must be carefully cleansed of proprietary government information to guard against inappropriate access. To prevent loss of privacy, media that are to be reused elsewhere within government must have data securely erased.

The destruction of information or disposition of diskettes containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE or Format function that does not result in the secure deletion of the data stored on the diskette; rather file and directory pointers are erased without ever touching the actual data. Data that is erased using the operating system DELETE/ERASE or Format function can be easily recovered.

Diskettes used by the Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the diskette disposal standard and procedure.

Standard

When diskette media is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed or securely erased using wiping software.

When diskette media is used to dispense licensed software, physical destruction of the media should occur in conjunction with the expiration of the software license.

If the media content is particularly sensitive, shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical

Roles and Responsibilities

Departments are responsible for physical destruction or secure wiping of all diskette media.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that diskette media has been disposed of in an appropriate fashion. There must be an audit trail that shows all diskette media has been physically destroyed, degaussed, or wiped at the appropriate time.

Procedure - Disposal of Diskettes

Methods for Secure Disposal

There are three primary methods for secure disposal of diskettes. Total destruction and degaussing are the two preferred methods. Secure erasure through wiping is a viable alternative but requires the purchase of wiping software.

Given the low cost of floppy diskettes the cost of wiping sensitive data from a diskette may not be justified. Degaussing or physical destruction of the diskette are both considered viable alternatives and recommended.

Other physical media such as ZIP Disks are more expensive than diskettes. However the cost of acquiring and using a wipe utility for ZIP cartridges may be cost prohibitive. Either degaussing or physical destruction through shredding are viable alternatives and recommended.

As a basic principle, all diskettes must be wiped each time they are to be employed by a new user. Given the cost and complexity of wiping diskette media care must be taken when sharing such media. Given the low cost of floppy media departments should consider using new media any time they are required to share data with a third party to prevent the accidental release of sensitive information.

Physical destruction of diskette media via drilling holes in the diskette, sanding, incineration, etc. is typically not recommended. Although these may be effective physical destruction methods, safety, environmental and/or health concerns preclude using such procedures. The only effective and safe method would be degaussing, or shredding of the media.

Government departments should consider the use of commercial shredding operations to safely destroy floppy diskettes or other removal storage media.

Disposal Standard for USB Memory Storage Devices

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of universal serial bus (USB) memory storage devices including disposal. For the purpose of this document the term USB memory storage device refers to any form of storage device that plugs into a USB port and uses non volatile memory to store data.

Before disposal all USB memory storage devices must be carefully cleansed of proprietary government information to guard against inappropriate access. To prevent loss of privacy all USB memory storage devices that are to be reused elsewhere within government must have data securely erased using wiping software.

The destruction of information or disposition of memory sticks containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE or Format function that does not result in the secure deletion of the data stored on the memory stick; rather file and directory pointers are erased without ever touching the actual data. Data that is erased using the operating system DELETE/ERASE or Format function can be easily recovered.

USB memory storage devices used within Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the USB memory storage device disposal standard and procedure.

Standard

When a USB memory storage device is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed or erased using wiping software.

USB memory storage devices must be securely erased prior to reuse in other departments, boards, agencies, or special operating agencies using wiping software.

If the media content is particularly sensitive, destruction through shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical

Roles and Responsibilities

Departments are responsible for physical destruction or wiping of all USB memory storage devices.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that USB memory storage media has been disposed of in an appropriate fashion. There must be an audit trail that shows all USB memory storage devices have been physically destroyed or wiped at the appropriate time.

Procedure - Disposal of USB Memory Storage Devices

Methods for Secure Disposal

There are two primary methods for secure disposal of information on USB memory storage devices, total destruction, and secure erasure through wiping. Secure erasure using wiping software may not be practical due to the cost of procuring wiping software capable of securely erasing the USB memory storage device.

As a basic principle, all USB memory storage devices should be wiped each time they are to be employed by a new user. Given the cost and complexity of wiping USB memory storage devices care must be taken when sharing such media with third parties. Departments should consider using alternative forms of electronic media such as CD or DVD media any time they are required to share data with a third party to prevent the accidental release of sensitive information.

Government departments should consider the use of commercial shredding operations to safely destroy USB memory storage devices that are no longer of use.

Appendix A
Sample Electronic Media Clearing Standards (RCMP)

The following are the RCMP standards for secure disposal of different media types.

Hard-Disk Drives/Diskette

Protected A/B/Confidential:

a) Run thru disintegrator/pulverizer to a maximum 7.5 cm./3-inch size or (incineration) or
b) (Internal reuse) One time software overwrite
(External reuse or disposal) Three time software overwrite

Protected C/Secret:

a) (Degauss or 3-time overwrite or pre-encrypt) and run thru a disintegrator/pulverizer to a maximum 7.5 cm./3-inch size or
b) Disintegrate to 6mm/¼ inch screen size or
c) incineration

Top Secret:

(Degauss or 3-time overwrite or pre-encrypt) and run thru a disintegrator to a maximum 3mm (1/8 inch size)

Optical Media (CD's, DVD's etc)

Protected A/B/Confidential:

Surface grinding or 1.5 cm (1/2 inch) maximum size residue Protected "C"/Top Secret/Secret: Surface grinding or 3X3 mm (1/8" X 1/8") particles (disintegration) or incineration

Integrated Circuit/Flash Memory

Includes: USB Memory sticks, RAM and "Flash ROM Memory" are non-volatile

Protected A/B/Confidential

One time overwrite or damage with hammer/pulverizer/heat/incineration

Protected C/Top Secret/Secret

Highly sensitive information should not be stored on these devices but in the special case that it was, contact RCMP or CSE for instructions

Tape Media

Protected A/B/Confidential:

1.5X 1.5 cm (½" X ½") particles (disintegration) or degaussing/incineration

Protected "C"/Top Secret/Secret:

3X3 mm (1/8" X 1/8") particles (disintegration) or degaussing/incineration

Appendix B
Definitions

Destruction – To alter the physical structure of the media so that the risk of unauthorized information disclosure is minimal. Physical destruction of media should be conducted by a commercial shredding operation.

Degaussing – An electronic purging procedure. Degaussing applies a reverse magnetic field to electronic media. This changes the magnetic lines of flux and reduces the magnetic induction to zero thus eliminating information from the electronic media.

Disposal – The release or transfer of magnetic storage media outside the control of the Government.

Multifunction Device – A multi function device is an electronic device that combines the functionality of multiple computer or electronic devices such as fax, photo copier, and printer into a single device.

Reuse - To redistribute and reassign storage media and its control to different environments

Sanitization - Generic term for removing sensitive information from storage media.

Secure Erase - To erase data using wiping techniques to eliminate data from the magnetic media. A secure erase can be used to erase a file, or to erase files that were not previously erased using a secure erase process.

Shredding – A means of destroying media by mechanically cutting the media into narrow strips.

Wiping - A standard overwrite technique used to erase sensitive data from a storage media. Wiping involves methods of writing 1's to the media, followed by writing 0's on top of the previous 1's. With each pass the chance of recovery is greatly reduced.

This is Schedule "C" to the Information Manager Agreement between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

CERTIFICATE OF DESTRUCTION OF INFORMATION

In accordance with subsection 6.06 of the Agreement, I _____ (Name and Position), certify the following:

1. On_____(Date), I destroyed all forms of the following Information, or I directed the destruction of the following information and I reasonably believe it will be destroyed, including all known copies, including back up copies and copies stored on computer hard drives or other portable media storage devices:

2. I have destroyed the Information, or I have directed the destruction of the Information and I reasonably believe it will be destroyed, in a manner that adequately protects the confidentiality of the Information and which is appropriate to the medium in which the Information was recorded, in a manner that makes it impossible to read or reconstruct the Information and in accordance with Schedule "C" of the Agreement and in accordance with applicable legislation. In particular, the following method of destruction was used:

Certified by: _____ _____

Officer's signature Position

Date:_____

This is Schedule "D" to the Information Manager Agreement

between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

SCHEDULE D – PLEDGE OF CONFIDENTIALITY

I ACKNOWLEDGE THAT I have reviewed the policies and procedures of 24-7 Intouch, Inc. on the collection, use, disclosure, protection, alteration, retention and destruction of personal health information and personal information (the "Information").

I UNDERSTAND THAT I am bound by the requirements of the Terms of Use Agreement and by the policies and procedures established by 24-7 Intouch, Inc. respecting the collection, use, disclosure, protection, accuracy, alteration, retention and destruction of the Information.

I UNDERTAKE AND AGREE THAT:

1. I will not collect, use, disclose, alter, retain or destroy the Information except in accordance with the Terms of Use Agreement and any applicable policies and procedures of 24-7 Intouch, Inc..

2. I will treat the Information to which I have access under the Terms of Use Agreement as strictly confidential and will use the Information solely for the purposes outlined in the Terms of Use Agreement and for no other purpose.

3. I will only access Information that I am authorized to use and that I need to know to carry out my work-related duties.

4. Except when necessary to carry out my work-related duties and in accordance with the Terms of Use Agreement document:

    a. I will not retain or make copies of any Information, in any form or medium, and

    b. I will not disclose or permit access to any Information, in any form or medium, to any person, corporation, organization or entity.

I ACKNOWLEDGE THAT failure to comply with the undertakings in this Pledge of Confidentiality may result in a breach of *The Personal Health Information Act* ("PHIA") and *The Freedom of Information and Protection of Privacy Act* that can result in disciplinary action up to and including dismissal, the imposition of a fine if found guilty of an offence under PHIA and, where applicable, a report to my health profession regulatory body.

Name (Printed)

Position

Signature

Date

Exhibit 3 – Information Sharing Agreement

INFORMATION SHARING AGREEMENT FOR ACCESS TO AND USE OF THE PUBLIC HEALTH INFORMATION MANAGEMENT SYSTEM (PHIMS)

BETWEEN:

THE GOVERNMENT OF MANITOBA,
as represented by the Minister of Health, Seniors and Active Living of Manitoba ("**Manitoba**")

and

24-7 Intouch, Inc.
"Organization"

WHEREAS:

A. the Manitoba Public Health Information Management System (PHIMS), formerly Panorama, involves an integrated, electronic public health record that improves and supports the delivery of population-level preventive interventions including, but not limited to, the surveillance and management of communicable disease cases and outbreaks, immunizations and vaccine inventory management;

B. The **Organization** has requested to access to PHIMS to provide services as outlined in an agreement between the Organization and Manitoba effective April 13, 2020 and a Statement of Work signed on November 24, 2020, namely COVID-19 case investigations, contact tracing and daily contact and follow up services ("**Agreement for Services**");

C. The **Organization** acknowledges that the use of and access to PHIMS will involve the transmission of Information between it and it's Authorized Users and **Manitoba** through the PHIMS Shared Service (Schedule D to this Agreement);

D. in order to ensure the confidentiality of the Information and to prevent from unauthorized access, collection, storage, use, disclosure, storage and destruction of the Information the Parties wish to enter into this Agreement;

NOW THEREFORE, the Parties agree as follows:

1 TERM OF THE AGREEMENT

1.1 This Agreement shall come into effect on the date it is signed by the last Party to do so, and will remain in effect until the date on which this Agreement is terminated pursuant to section 18.

2 DEFINITIONS, INTERPRETATION AND SCHEDULES

2.1 Capitalized terms in this Agreement have the following meanings:

(a) "Agreement" means this Information Sharing Agreement, including the recitals and any schedules to this Agreement, as amended from time to time;

(b) "Authorized Organization" means an organization or entity with whom Manitoba has entered into an agreement in order to facilitate access the PHIMS Service by that organization's or entity's employees, agents or contractors for an authorized purpose;

(c) "Authorized Use" means use of the Information by an Authorized User in accordance with the terms and conditions of this Agreement;

(d) "Authorized User" means a designated Representative of **Organization** who is permitted to access, use or disclose Information in the PHIMS Database through the PHIMS Service under the terms and conditions of this Agreement;

(e) "Business Day" means every day except Saturdays, Sundays and statutory holidays in the Province of Manitoba;

(f) "Confidential Information" means any information obtained in confidence from and deemed to be confidential by the Parties. The confidentiality of the Confidential Information is maintained in compliance with FIPPA, PHIA, the terms and conditions of this Agreement and any other laws and policies that apply to the Parties

(g) "Disclosure Directive" means the mechanism that allows individuals to request their Personal Health Information contained in the PHIMS Database not be disclosed to other health care providers;

(h) "FIPPA" means *The Freedom of Information and Protection of Privacy Act*, C.C.S.M. c. F175 and the regulations under that Act, as the Act or regulations may be amended from time to time;

(i) "Health Care" has the meaning given to that term in PHIA;

(j) "Information" means information, including Personal Health Information and, Personal Information, and Confidential Information, maintained in, and collected for the purpose of populating the PHIMS Database;

(k) "Information Manager" means Shared Health Inc., operating as Digital Health, the organization operating and administering PHIMS and the PHIMS Shared Service on behalf of **Manitoba**, and providing other information management and information technology services to **Manitoba**, for PHIMS;

(l) "Misuse" means any access, use, disclosure, retention or destruction of the Information by an Authorized User that is not in accordance with this Agreement, the Terms of Use for **Organization's** Authorized Users (Terms of Use attached as Schedule "A"), PHIMS Designation Guidelines, Report User Guides and each Party's respective written policies and procedures relating to the Information referred to in section 9 "Protection of The Information and Security Arrangements" of this Agreement;

(m) "Public Health Information Management System or "PHIMS" means the most current release of the software called "Panorama" in use by Manitoba during the course of the Agreement, consisting of, for the purposes of the Agreement, the Immunization Management and Materials/Vaccine Inventory Management, Investigations (which includes Communicable Diseases and Rh Surveillance) modules and related shared

services, along with all releases, hot fixes, enhancements, modifications and improvements to PHIMS made from time to time;

(n) "PHIMS Database" means the electronic database maintained by **Manitoba** for the purpose of PHIMS;

(o) "PHIMS Designation Guidelines" means the guidelines describing the requirements respecting the assignment of User Roles to Authorized Users;

(p) "PHIMS Shared Service" means the viewable, printable and searchable computer application and technical support services that provide Authorized Users with secure real-time access to Information in the PHIMS Database;

(q) "PHIMS System Updates" means the regular communication sent by email from the Information Manager to Authorized Users and those RHA Representatives responsible for designating Authorized Users and assigning User Roles;

(r) "Parties" means **Manitoba** and the **Organization**;

(s) "Party" means any one of **Manitoba** or the **Organization**;

(t) "Personal Health Information" has the meaning given to that term in PHIA;

(u) "Personal Information" means information about an identifiable individual as defined in *The Freedom of Information and Protection of Privacy Act*, C.C.S.M. c. F175 (Manitoba);

(v) "PHIA" means *The Personal Health Information Act*, C.C.S.M. c. P33.5 and the regulations under that Act, as the Act or regulations may be amended from time to time;

(w) "*Public Health Act*" means *The Public Health Act,* C.C.S.M. c. P210, and the regulations under that Act, as the Act or regulations may be amended from time to time;

(x) "Representative" means a Party's employees, agents, or contractors and any other person for whom the Party is responsible at law;

(y) "Services" means activities and responsibilities of **Manitoba** or the **Organization** as outlined in this Agreement;

(z) "Third Party" means an individual, corporation, organization or entity other than **Manitoba** and the **Organization** or a Representative of either Manitoba or the **Organization**;

(aa) "Trustee" has the meaning given to that term in PHIA; and

(aa) "User Role" means the specific role or roles to which an Authorized User is assigned and which prescribes what Information the Authorized User is permitted to access, use and disclose.

2.2 Unless specifically stated otherwise in this Agreement:

(a) words and phrases denoting inclusiveness (such as "including" or "includes"), whether or not stated as being without limitation, are not limited by their context or the words or phrases which precede or succeed them;

(b) where the Agreement, approval or consent of a Party is required, it will be in writing and will not be unreasonably withheld or delayed; and

(c) whenever the words discretion, option, determine, election or other similar words or any variation thereof are used with respect to a Party, they will be deemed to mean such Party's sole and absolute discretion, option, determination, election or other such similar act.

2.3 No provision of the Agreement shall be interpreted against any Party merely because that Party or its legal representative drafted the provision.

2.4 In interpreting this Agreement:

(a) where required by context, words in the singular include the plural and words in the plural include the singular; and

(b) the headings in this Agreement are for convenience of reference only and shall not affect the scope, intent or interpretation of any provision of this Agreement.

2.5 The preamble and following schedules form part of this Agreement:

(a) Schedule "A" – PHIMS Terms of Use

(b) Schedule "B" – Pledge of Confidentiality;

(c) Schedule "C" – Electronic Media Disposal Standards and Procedures;

(d) Schedule "D" – PHIMS System Services and Related Services; and

(e) Schedule "E" – Certificate of Destruction.

3 PURPOSE OF THIS AGREEMENT

3.1 This Agreement establishes the terms and conditions under which the **Organization's** Authorized Users will be provided with access to the PHIMS Shared Service.

3.2 **The Organization's** Authorized Users will be permitted to access, use or disclose the Information in the PHIMS Database through the PHIMS Service only in accordance with their User Role and as required to perform the Services pursuant to the Agreement to assist Manitoba in responding to the COVID-19 Pandemic, including for the following purposes:

(a) to conduct COVID-19 case investigations;

(b) to provide contact tracing services; and

(c) to provide daily case contact and follow up or referral services.

3.3 The Organization acknowledges and agrees that access to, use or disclosure of the Information in the PHIMS Database by the Organization's Authorized Users through the PHIMS Shared Service is for the purposes set out in section 3.2 of this Agreement only and for no other purpose.

4 INFORMATION SHARING

4.1 In compliance with FIPPA and PHIA and pursuant to the terms and conditions of this Agreement **Manitoba** will provide **the Organization** with access to the Information described in subsection

4.2 for the authorized purposes set out in subsection 3.2.

5 CUSTODY, CONTROL AND MAINTENANCE OF INFORMATION

5.1 The **Organization** acknowledges and agrees that, for the purposes of FIPPA, **Manitoba** has custody and control of all the Information in the PHIMS Database.

5.2 The **Organization** acknowledges and agrees that, for the purposes of PHIA, **Manitoba** maintains all the Information in the PHIMS Database as a Trustee.

5.3 Nothing in this Agreement confers on the **Organization** or its Authorized Users any title to or right or interest in any of the Information in the PHIMS Database and neither deprives the **Organization** nor any of its Authorized Users of any right, title or interest they may have by virtue of applicable law.

6 CONFIDENTIALITY AND PRIVACY PROVISIONS

6.1 The **Organization** agrees that its Authorized Users will only access, use or disclose the Information through the PHIMS Shared Service to carry out the authorized purposes under subsection 3.2 of this Agreement and the Organization shall take reasonable steps to ensure that their Authorized Users do not Misuse Information.

6.2 The **Organization** shall take reasonable steps to ensure that no persons, other than its Authorized Users:

(a) acquire access to Information in the PHIMS Database;

(b) remove any Information, or any copy of the Information, in any form or medium;

(c) retain or make unauthorized copies of the Information, in any form or medium;

(d) modify or alter any Information in any manner except as required to accurately populate and update the PHIMS Database;

(e) link or match the Information with any other Information, except to the extent necessary to carry out the Authorized Purposes in subsection 3.2 of this Agreement.

6.3 The **Organization** shall take reasonable steps to ensure that their Authorized Users:

(a) treat the Information as strictly confidential;

(b) are aware of, and complies with:

i. the requirements, obligations and procedures respecting the collection, use, protection, retention, disclosure, alteration and destruction of, and access to, the Information in PHIA and FIPPA, as applicable to the Information and the Authorized User,

ii. the requirements and obligations of this Agreement,

iii. the criteria and requirements outlined in the PHIMS Designation Guidelines and Report User Guides, as amended, revised or changed by **Manitoba** in accordance

with this Agreement from time to time,

iv. the privacy and security policies, procedures, safeguards and measures of **Manitoba** or **the Organization** as applicable to the Authorized User,

v. any additional reasonable requirements or directions established or given by **Manitoba** to safeguard or ensure the confidentiality of the Information or to protect the privacy of the individuals the Information is about; and

(c) is aware of the consequences of breaching:

i. the requirements and obligations in PHIA and FIPPA, as applicable to the Authorized User,

ii. the requirements and obligations in this Agreement and the Report User Guides, and

iii. **Manitoba's** or the **Organization's** privacy and security policies, procedures, safeguards and measures as applicable to the Authorized User

6.4 The **Organization** shall comply with all applicable laws, regulations and policies relating to the protection, management, security and privacy of the Information.

7 DESIGNATION OF AUTHORIZED USERS

7.1 The Organization shall:

(a) appoint a designated employee of the Organization who shall have the responsibilities in subsection 7.2 below;

(b) provide the Information Manager with the names and contact information of the designated employee referred to in subsection 7.1;

(c) promptly notify the Information Manager as to any change to the identity of the designated employee referred to in subsection 7.1 and any changes to their contact information.

7.2 The **Organization's** designate will be responsible for:

(a) designating the Representatives of the Organization who will be Authorized Users in accordance with the conditions and requirements of the Agreement;

(b) assigning User Roles to Authorized Users in accordance with the conditions and requirements of the PHIMS Designation Guidelines;

(c) ensuring that **Manitoba**'s Information Manager is notified of any changes that require user accounts to be disabled or modified due to changes in User Role or employment or contractual responsibilities;

(d) ensuring all Authorized Users receive training and have access to support materials, including training and support materials accessible on the PHIMS website, before using PHIMS;

(e) reviewing and, where applicable complying with, all the PHIMS System Updates that are sent from the Service Desk; and

(f) reviewing a list of Authorized Users, provided by **Manitoba**'s Information Manager at a minimum of once per year, or when directed by **Manitoba**, to confirm the Authorized Users listed continue to require access to the Information through the PHIMS Shared Service for an authorized purpose under subsection 3.2 of this Agreement and the accuracy of their assigned User Roles.

7.3 The Organization shall:

(a) Only designate Authorized Users that:

i. are Representatives of the **Organization**; and

ii. need to know or require access to the Information through the PHIMS System Service in order to carry out an authorized purpose under subsection 3.2 of this Agreement in the performance of his or her employment duties or contractual obligations, as determined by the **Organization**.

(b) only assign the minimum number of Authorized Users to User Roles as necessary in accordance with the PHIMS Designation Guidelines;

(c) not assign an Authorized User a User Role if the assignment would exceed the User Role limit specified in the PHIMS Designation Guidelines, unless Manitoba provides prior written approval;

(d) only assign a User Role:

i. that corresponds to or is consistent with the Authorized User's employment duties or contractual obligations; and

ii. for which the Authorized User is qualified.

(e) The **Organization** acknowledges that a description of the required qualifications for each User Role is set out in the PHIMS Designation Guidelines.

7.4 Subject to subsection 8.2 of this Agreement, the **Organization** shall designate Authorized Users and their assigned User Roles in writing and shall provide this information to **Manitoba's** Information Manager.

7.5 The **Organization** will direct its Authorized Users to agree to the Terms of Use in either a hardcopy or electronic-based format, as determined and directed by Manitoba and submit the Terms of Use to Manitoba's Information Manager in the required format.

7.6 The **Organization** acknowledges and agrees that **Manitoba** will provide an individual, on request, with access to the names of the **Organization's** Authorized Users or Representatives who have accessed the individual's Information through the PHIMS Shared Service in accordance with the Ministerial Guidelines for Records of User Activity established pursuant to the Personal Health Information Regulation under PHIA.

7.7 If an Authorized User

(a) is no longer a Representative of the **Organization** or is no longer carrying out the employment or contract-related activities, duties or tasks that require access to the PHIMS Service, as required under subsection 7.2 of this Agreement; or

(b) is in breach of his or her Terms of Use or Pledge of Confidentiality (where applicable), or the requirements, directions, privacy policies or procedures or security safeguards and measures established by the **Organization** or **Manitoba** or

(c) is responsible for any Misuse,

Manitoba or the Organization shall revoke **Organization's** Authorized User's designation as an Authorized User, and the shall promptly notify **Manitoba's** Information Manager in writing of the revocation and take reasonable steps to ensure that the Authorized User ceases to have any access to the Information.

7.8 Where Manitoba has revoked the Authorized User's designation of one of the RHA's Authorized Users, Manitoba will notify the Organization of the revocation and provide a written rationale if requested by the Organization.

7.9 **Manitoba** may terminate an Authorized User's access to the PHIMS Service if, in the opinion of Manitoba, the Authorized User is responsible for any Misuse of the Information.

8 AUTHORIZED ACCESS TO, USE OR DISCLOSURE OF INFORMATION

8.1 **Manitoba,** through its Information Manager, agrees to provide access to the Information through the PHIMS Service to the **Organization's** Authorized Users for the purposes set out in Section
3.2 of the Agreement.

8.2 The **Organization** acknowledges and agrees that access to, use, or disclosure of Information through the PHIMS Shared Service will be limited to the **Organization's** Representatives who:

(a) are designated by the **Organization** in writing and in accordance with section 7, as being authorized to access, use or disclose the Information; and

(b) have signed or completed a Pledge of Confidentiality that includes an acknowledgement that he or she has reviewed and is bound by **Organization's** written policies and procedures respecting access to, use, disclosure, storage, accuracy, protection and security of the Information, and is aware of the consequences of breaching them. A Pledge of Confidentiality is attached as Schedule B.

8.3 In addition to the requirements set out in subsections 8.2(a) and (b), the **Organization** acknowledges and agrees that access to, use or disclosure of the Information through the PHIMS Shared Service with respect to the **Organization's** Representatives will be limited to those Representatives who have been designated as Authorized Users and have executed the Terms of Use attached as Schedule "A".

8.4 Subject to the requirements under subsection 8.3, the **Organization** shall provide its Authorized Users with designated desktop or laptop computers and other necessary hardware and software owned by or licensed to the **Organization** to securely access the PHIMS Shared Service.

8.5 The **Organization** acknowledges and agrees that its Authorized Users will access the PHIMS Shared Service using a unique username and password.

8.6 The **Organization** must direct their Authorized Users to not use personal computers or other electronic devices to access the PHIMS Shared Service, and must take reasonable steps that such activity does not occur unless Manitoba approves otherwise in writing.

8.7 The **Organization** and **Manitoba** shall take all reasonable efforts to maintain the quality and integrity of the Information. However, the **Organization** acknowledges that **Manitoba** cannot warrant the accuracy or completeness of the Information accessed through the PHIMS Shared Service where this is dependent on factors beyond the control of **Manitoba**, including but not limited to, data quality and integrity from the data source and revisions or alterations by Authorized Users. The **Organization** shall be responsible to maintain the quality and integrity of data that is inputted into the PHIMS Database by the **Organization's** Authorized Users.

9 PROTECTION OF THE INFORMATION AND SECURITY ARRANGEMENTS

9.1 **Manitoba** acknowledges its responsibility as a Trustee of the Information maintained in the PHIMS Database and agrees to protect the Information from unauthorized access, collection, use, disclosure, retention and destruction in accordance with the requirements under PHIA, FIPPA and **Manitoba's** written policies and procedures.

9.2 Without limiting the generality of subsection 9.1, **Manitoba** shall ensure that access to and use of Information contained in the PHIMS Database by its Authorized Users is:

(a) limited to Authorized Users who have been authorized to access or use the Information and have a need to know the Information; and

(b) limited to the minimum amount of Information necessary to accomplish the authorized purposes for which the Information is accessed or used.

(c) limited to those Authorized Users who have completed mandatory PHIA training provided by the Manitoba Department of Health, Seniors and Active Living, and signed a Pledge of Confidentiality

9.3 The **Organization** shall establish, or have established, and comply with written policies and procedures respecting access to, use, disclosure, storage, accuracy, protection and security of the Information that are consistent with and reflect the requirements of this Agreement, applicable laws.

9.4 Without limiting the generality of subsection 9.3, the **Organization's** respective written policies and procedures shall include:

(a) a requirement that no record of the Information shall be removed from PHIMS;

(b) measures to protect the security of Information in electronic form when the computer hardware (including laptops) or portable electronic storage media (including USB memory devices) on which it has been recorded is being disposed of or used for another purpose;

(c) provisions for the recording of privacy and security breaches; and corrective procedures to address privacy and security breaches.

9.5 The **Organization** shall put in place security safeguards, including administrative, technical, operational and physical safeguards that protect the confidentiality and security of the Information, and protect the Information against Misuse, and against such risks as unauthorized access, use, disclosure, alteration and retention of the Information by other Representatives and Third Parties.

9.6 Without limiting subsection 9.5, as a minimum, the **Organization** shall comply with the following

security safeguards, in addition to those prescribed in Exhibit 4 to the Agreement for Services (Personnel and Security Requirements):

(a) The **Organization** shall implement controls that:

i. limit access to the PHIMS Shared Service and Information in the PHIMS Database to only Authorized Users in their assigned User Roles, and

ii. ensure that the PHIMS Service and Information in the PHIMS Database is accessed, used, or disclosed only by persons who are verified as Authorized Users in an assigned User Role who are making use of same for an authorized purpose under subsection 3.2 of this Agreement; and

iii. ensure that it only approves devices that Authorized Users may use to access the PHIMS Service that are secure, not available for public use , have suitable anti virus and spyware protections and meet the requirements of this Agreement.

(b) The **Organization's** information technology systems shall include reasonable hardware, software and procedural security control measures, designed to prevent the following:

i. unauthorized access and systematic attempts to disrupt service;

ii. unauthorized changes to software and hardware components;

iii. propagation and execution of harmful code, including but not limited to computer viruses and malware; and

iv. unauthorized access to and disclosure of the Information.

(c) The **Organization** must ensure that a tracking mechanism is in place that records the serial number of the computing hardware used to access the PHIMS Service (including laptop and desktop computers, and portable electronic storage media) and the resource to which it was given to facilitate recovery of the hardware if it is lost or misplaced.

(d) The **Organization's** Authorized Users will have installed and operate the following security controls on their desktop and laptop computers:

i. operating system password settings;

ii. a password protected keyboard/screen lock that is automatically activated by a period of inactivity of no more than twenty (20) minutes; and

iii. personal firewall and anti-virus and anti-malware programs.

(e) The **Organization's** Authorized Users will have installed and operate encryption software capable of encrypting Information stored on laptop computers and portable electronic storage media (including USB memory devices).

(f) The **Organization** must require their Authorized Users to encrypt all Information stored electronically when:

i. the Information is in transit and at rest on an Authorized User's laptop or approved device; and

ii. the Information is being transmitted.

(g) Where Information is stored on the **Organization's** premises or on Authorized Users' computers, then at all times access to such premises and computers must be controlled to exclude access by unauthorized individuals. In addition:

i. the Authorized User in possession of Information must be required to lock his or her office, when they leave for the balance of the day; and

ii. where the Authorized User is in possession of Information cannot lock their office, when leaving for the balance of the day they must be required to:

1. power down the computer or device such that it cannot be used unless a password is required as part of re-starting the computer, or, where the device is not to be powered down, activating the password protected keyboard/screen lock;

2. lock all paper records or portable media storage devices containing Information that are being left on the premises in a secure desk, filing cabinet or room; and

3. when an Authorized User works remotely or outside of his or her office and is in possession of Information stored on a laptop or portable media storage device, the Authorized User must be instructed and required to never leave the laptop computer or portable media storage device unattended, unless it is physically locked in a secure desk, filing cabinet or room, or secured by cable lock.

9.7 In addition to complying with the requirements in this Agreement, the **Organization** shall comply with any additional reasonable requirements established by **Manitoba** from time to time to protect the Information.

9.8 The **Organization** shall provide orientation and periodic training for its Authorized Users about the requirements of FIPPA, PHIA, this Agreement, the Terms of Use and about the **Organization's** written policies and procedures at least once every three (3) years.

9.9 As **Manitoba** makes available any training or education on the use of the PHIMS Shared Service and the protection of Information in the PHIMS Database, or relating to any other obligation of the **Organization** or its Authorized Users under this Agreement, and if so requested by **Manitoba**, the **Organization** shall make said material available to its Authorized Users and cause its Authorized Users to participate in such training or education.

10 RECORDS

10.1 While this Agreement is in effect, the **Organization** shall maintain the following records and shall provide **Manitoba's** Information Manager with copies of these records as soon as practicable upon request:

(a) records confirming that an Authorized User has signed or completed a Pledge of Confidentiality required under subsection 8.2(b) of this Agreement and Terms of Use executed by Authorized Users;

(b) a list of names of the **Organization's** Authorized Users and the User Roles to which they

have been assigned in accordance with section 7 of the agreement;

(c) records of the **Organization's** security and privacy policies and procedures; and

(d) reports of all security and privacy breaches and corrective procedures put in place, as required under subsections 9.4(c) of this Agreement.

11 REPORTS RESPECTING THE INFORMATION

11.1 The **Organization** shall, immediately upon becoming aware of any of the following, notify **Manitoba** in writing of:

(a) any Misuse of the Information, or other any unauthorized access to, use, disclosure, alteration or retention of the Information by another Representative or Third Party; and

(b) any breach (actual or threatened) of any term or condition of this Agreement or the Terms of Use executed by an Authorized User,

with complete details of the incident. The **Organization** shall immediately take all reasonable steps to prevent the recurrence of any Misuse, or other unauthorized access to, use, disclosure, alteration and retention of the Information, or to remedy the breach in a manner satisfactory to **Manitoba**, and shall promptly, and in writing, notify **Manitoba** of the steps taken.

12 INVESTIGATIONS, REVIEWS AND AUDITS

12.1 Manitoba will in accordance with PHIA and Ministerial Guidelines approved under PHIA, establish auditing processes and procedures to monitor and review Authorized Users' access to and use of the PHIMS Shared Service.

12.2 The **Organization** acknowledges and agrees that **Manitoba** will generate audit reports, in a form and with the contents as determined by **Manitoba** ("Audit Reports"), and provide those reports to **Organization** about the activities of the **Organizations** Authorized Users as part of routine auditing processes, or when possible Misuse is detected. The **Organization** agrees to protect the Information contained in Audit Reports disclosed by **Manitoba** in accordance with any applicable requirements or obligations set out in this Agreement.

12.3 **Manitoba** may, at its discretion and acting reasonably, develop guidelines for the assessment and review of Audit Reports by the **Organization**, which will be communicated to the **Organization**. The **Organization** shall comply with any such guidelines.

12.4 The **Organization** shall conduct any reviews, audits and investigations relevant to the activities of the **Organization's** Authorized Users as and when necessary to ensure compliance with the **Organization's** and their Authorized Users' obligations under this Agreement. In addition, the **Organization** shall take reasonable steps to remedy any deficiencies identified by the review, audits and investigations, administer any sanctions deemed appropriate by the **Organization** and promptly notify **Manitoba's** Information Manager in writing as to the remedial measures taken.

12.5 When requested by **Manitoba**, the **Organization** agrees to carry out a review of the **Organization's** information practices as they relate to access to, use, disclosure, retention, protection, security and destruction of the Information. The **Organization** shall provide copies of the results of any review to **Manitoba** within twenty-four (24) hours of completing the review.

12.6 Upon reasonable advanced written notice, **Manitoba** or its agents may carry out inspections or audits of the **Organization's** security practices involving the Information as **Manitoba**, acting reasonably, considers necessary to ensure the adequate protection of the Information and to monitor compliance with this Agreement and Terms of Use Agreements.

12.7 The **Organization** must cooperate in any assessment, review or audit carried out by **Manitoba** or its agents. In addition, the **Organization** must permit access, at all reasonable times, to their premises, records and information in order to carry out such assessments and audits and to ensure compliance with this Agreement.

12.8 The **Organization** shall provide a copy of the results of an internal audit, and any related action plans, to **Manitoba** within twenty-four (24) hours of completing the audit.

12.9 If any inspection, review or audit identifies deficiencies in the Organization's practices regarding the Information, the Organization must take reasonable steps, acceptable to Manitoba, to correct the deficiencies immediately and shall promptly notify Manitoba's Information Manager in writing as to the steps taken.

13 OBLIGATIONS TO ASSIST INDIVIDUALS THE INFORMATION IS ABOUT

13.1 The **Organization**, through its Authorized Users, shall:

(a) assist individuals to view their Information by redirecting requests from individuals to view their Information to **Manitoba**;

(b) assist individuals with inquiries regarding the disclosure of their Information, corrections, access requests, and requests to see who has accessed or viewed their Information by directing them to Manitoba.

14 DESTRUCTION OF INFORMATION

14.1 The **Organization** shall, immediately upon the earlier of a request by **Manitoba** or the termination of this Agreement ensure its Authorized Users refrain from any further access to, use and disclosure of, or transactions involving the Information, in any form whatsoever. The **Organization** shall also destroy all forms of the Information, including all known copies, including copies stored on computer hard drives or other portable media storage devices, in a manner that makes it impossible to read or reconstruct the Information.

14.2 Without limiting the generality of subsection 14.1, all magnetic computer tapes, compact disks, diskettes, computer hard drives, USB memory devices and other portable media storage devices shall be disposed of following practices consistent with the Manitoba Government Electronic Media Disposal Standards and Procedures, a copy of which is attached to this Agreement as Schedule "C".

14.3 The **Organization** shall provide written confirmation of the destruction of the Information to Manitoba including a general description of the Information destroyed, the date of destruction, the method of destruction and the person responsible for the destruction, in the form attached as Schedule "E".

15 PHIMS SYSTEM SERVICES AND RELATED SERVICES

15.1 Organization agrees to accept and Manitoba, through its Information Manager, agrees to

provide, the Services as outlined in Schedule "D", in accordance with the terms, conditions, roles and responsibilities set out in this Agreement.

16 TERMINATION

16.1 Notwithstanding Section 1 **Manitoba** may, subject to section 19, immediately terminate this Agreement if:

(a) **Manitoba**, in its sole opinion, concludes that:

i. the Information was accessed, used, disclosed, altered or, retained by the **Organization**, an **Organization**'s Representative (other than an Authorized User) or a Third Party in a manner which is not authorized under this Agreement;

ii. the **Organization** has not protected the Information from unauthorized access, use, disclosure, alteration, or retention in accordance with this Agreement, applicable legislation and the **Organization's** protocols and policies; or

iii. the nature and magnitude, or number or frequency of Misuses by an Authorized User is such that **Manitoba** loses faith in the **Organization's** ability to protect the Information in accordance with this Agreement; or

(b) **Manitoba's** Agreement with its Information Manager is terminated

16.2 On termination of this Agreement the **Organization** shall ensure that its Authorized Users immediately refrain from further accessing the PHIMS Shared Service. The termination of this Agreement in no way releases the **Organization** from its obligations to protect the Information.

17 GENERAL

17.1 The main body of this Agreement may be amended at any time as the Parties, as represented by the persons occupying the positions of signatories to this Agreement, agree in writing.

17.2 Any of the Schedules to this Agreement may be amended at any time as the Parties agree through an exchange of letters between the designated officials for Manitoba and the **Organization** listed in section 18 of this Agreement. The amendment will come into effect on the date of last signing of the letter.

17.3 The **Organization** shall not assign or transfer this Agreement or any of the rights or obligations under this Agreement. without first obtaining written permission from **Manitoba**.

17.4 This Agreement shall be governed and construed in accordance with the laws in force in the Province of Manitoba.

17.5 The Parties agree to give one another notice as soon as reasonably possible in writing of any change in their policies, programs or information which is likely to affect this Agreement or any of its schedules.

17.6 No term or condition of this Agreement shall be deemed to be waived and no breach or omission excused, unless the waiver is in writing and signed by the Party granting the waiver.

17.7 The obligations of the **Organization** set out in this Agreement relating to Authorized Users continue even if the individual ceases to be an Authorized User of the **Organization** or ceases

to be a Representative of the **Organization**. Without limiting the generality of the foregoing, the Organization's obligations under subsection 12.4 continue to apply in relation to those individuals who cease to be Authorized Users or Representatives of the Organization and the obligation under subsection 11.1 continues to apply to those individuals who cease to be Authorized Users or Representatives of the Organization.

17.8 Those sections that by their very nature are intended to survive the termination or expiration of this Agreement shall survive the expiration or termination of this Agreement. Without limiting the foregoing, the termination of this Agreement in no way releases the Organization from its obligations to protect the Information.

17.9 In no event will either Party, or their officers, employees or agents, be liable to the other Party for any costs, damages, claims, liabilities or demands, including any claims, liabilities or demands with respect to any injury to persons (including, without limitation, death), damage or loss to property, economic loss or incidental or consequential damages or infringement of intellectual property rights, arising directly or indirectly from:

(a) any error, omission or defect in any Information provided under this Agreement;

(b) the other Party's use of, or inability to use, any Information provided under this Agreement;

(c) any disclosure of, or failure to disclose, Information under this Agreement; or

(d) any delay or failure to provide Information under this Agreement,

unless based upon, arising out of, relating to, occasioned by or attributed to the Party's gross negligence or willful misconduct.

18 NOTIFICATION

18.1 The **Parties** will give notice to each other in person, by mail, email, by courier or by facsimile to the following addresses:

Manitoba at:

Manitoba Health, Seniors and Active Living
Attention: Executive Director, Public Health Branch
4th Floor – 300 Carlton Street
Winnipeg, MB R3B 3M9
Phone: (204) 788-6781
Fax: (204) 948-2040

24-7 Intouch, Inc. at:

17(1) & 17(3)(e) [redacted]

[redacted]

Shared Health Inc. **(Information Manager)** at:

Shared Health

Attention: Director, Community and Long Term Care

17(1) & 17(3)(e) [redacted]

18.2 The date of receipt of any notice shall be deemed to be:

(a) the date of delivery of such notice if served personally, or via facsimile or email on a Business Day between the hours of 8:30 a.m. and 4:30 p.m., and if served outside the hours of 8:30 a.m. and 4:30 p.m., then the next Business Day; or

(b) if mailed, the third Business Day following the date of mailing; or

(c) if sent by overnight delivery by courier that has the ability to track deliveries and confirm receipts, then the next Business Day.

19 DISPUTE RESOLUTION

19.1 Notwithstanding Section 18 (Termination), any dispute between the Parties arising from the interpretation or application of this Agreement may, at the discretion of the Parties, be dealt with through negotiations between the Parties.

20 EXECUTION

20.1 The Parties may execute this Agreement in separate counterparts, each of which when so executed and delivered shall be an original. All such counterparts may be delivered by email of scanned document or facsimile transmission, and such transmission shall be considered an original.

26 [redacted]

IN WITNESS WHEREOF the Parties have executed this Agreement on the dates noted below.

GOVERNMENT OF MANITOBA
(as represented by _____)

Date: NOV 2 4 2020

17(1) & 17(3)(e) [redacted]

Karen Herd
Name

Deputy Minister
Title

24-7 Intouch, Inc.

Date: Nov-24-2020

17(1) & 17(3)(e) [redacted]
Authorized Signature

Mitul Kotecha
Name

President
Title

This is Schedule "A" to the Information Sharing Agreement for Access to and Use of the Public Health Information Management System (PHIMS)

between Manitoba and **24-7 Intouch, Inc.** **(the "Agreement")**

(insert name of Organization)

SCHEDULE A – PHIMS TERMS OF USE

In return for being authorized to access and use PHIMS (formerly Panorama), I agree to comply with the following Terms of Use:

1. Definitions

1.1 "Authorized Organization" means an organization or entity with whom Manitoba has entered into an agreement in order to facilitate access to the PHIMS by that organization's or entity's employees, agents or contractors for an authorized purpose;

1.2 "Authorized User" means a designated representative of the Authorized Organization permitted to access, use or disclose Information in the PHIMS application under the terms and conditions of this Agreement;

1.3 "FIPPA" means The Freedom of Information and Protection of Privacy Act, C.C.S.M. a. F175 and the regulations under that Act, as the Act or regulations may be amended from time to time;

1.4 "Information" means information, including Personal Health Information, Personal Information, and Confidential Information, maintained in, and collected for the purpose of populating the PHIMS Database;

1.5 "Information Manager" means Shared Health Inc., operating as Digital Health, the organization operating and administering PHIMS on behalf of **Manitoba**, and providing other information management and information technology services to **Manitoba**, for PHIMS and technical support services to Authorized Users of PHIMS.

1.6 "Public Health Information Management System" or "PHIMS" means the most current release of the software called "Panorama" in use by Manitoba during the course of the Agreement, consisting of, for the purposes of the Agreement, the Immunization Management, Materials/Vaccine Inventory Management, Investigations (which includes Communicable Diseases and Rh Surveillance) modules and related shared services, along with all releases, hot fixes, enhancements, modifications and improvements to PHIMS made from time to time;

1.7 "Personal Health Information" has the meaning given to that term in PHIA;

1.8 "PHIA" means *The Personal Health Information Act*, C.C.S.M. c. P33.5 and the regulations under that Act, as the Act or regulations may be amended from time to time;

1.9 "Personal Information" has the meaning given to that term in FIPPA;

1.10 "User Role" means the specific role or roles to which an Authorized User is assigned and which prescribes what Information the Authorized User is permitted to access, use and disclose.

2. Access to PHIMS (Panorama)

2.1. I understand that my PHIMS access privileges and assigned User Role(s), as authorized by my Authorized Organization, I am employed by or contracted to, are to be used only as required to perform my employment duties or contractual obligations.

2.2. I will only access, use or disclose the Information contained in PHIMS for the following authorized purposes of the Agreement:

(a) to provide Health Care or for arranging for the provision of health care;

(b) administrative responsibilities and duties related to supporting the provision of health care or arranging for the provision of Health Care;

(c) to generate Standard Reports as described in Schedule "F" and as prescribed in the Report User Guides;

(d) analysis of surveillance data to inform timely public health action and response and;

(e) to fulfil responsibilities and duties under *The Public Health Act.*

2.3. In addition to the authorized uses listed above, if I am representative of the Information Manager, I will only access PHIMS as authorized by Shared Health Inc to perform my employment duties.

2.4. I will only access, use or disclose the minimum amount of Information necessary to accomplish the authorized purposes for which the Information is accessed or used.

2.5. I agree not to disclose any Information contained in PHIMS to any person, other than to individuals the information is about and with whom I am in a care relationship. I agree that where I receive any other request for disclosure of information from PHIMSI must direct that request to Manitoba Health, Seniors and Active Living ("Manitoba Health"), Legislative Unit, at 204-788-6612, fax 204-945-1020, or email PHIAinfo@gov.mb.ca

2.6. In order to maintain a user account with PHIMS, I will provide to my Authorized Organization, and keep up-to-date, certain business contact information about me. I consent to that information being shared with Manitoba Health and its representatives, including its Information Manager.

2.7. I understand that my Authorized Organization may have its own policies and procedures for my access to and use of PHIMS, and I agree that I will comply with them as they may apply to me.

2.8. I understand that my activities as an Authorized User are subject to applicable laws and policies, including any relevant policies and procedures of my Authorized Organization.

2.9. I understand that I am still responsible for recording immunization information in the clinical records of my Authorized Organization where applicable and as required. This is in addition to disclosing information to and obtaining information from the PHIMS.

2.10. I acknowledge that my Authorized Organization will have control of the Information accessed from PHIMS that is maintained in my Authorized Organization's clinical client records and any other records maintained by my Authorized Organization in accordance with the Agreement, and that such information may fall under the purview of laws and policies applicable to my Authorized Organization.

3. Provision of PHIMS

3.1. I recognize that the Information presented through PHIMS may not be complete, as this is dependent on factors beyond the control of Manitoba Health and its representatives.

3.2. I acknowledge that the content, format and nature of PHIMS may change from time to time without prior notice to me.

3.3. I acknowledge that I will review, and where applicable comply with, the PHIMS System Updates and PHIMS Memos that are sent to me from the PHIMS Application Support team as they contain important PHIMS information.

3.4. I acknowledge that Manitoba Health in its sole discretion, acting reasonably and without prior notice, may temporarily or permanently cease making PHIMS, or any of its features, available to me or to users generally.

4. My password and account security

4.1. I am responsible for maintaining at all times the confidentiality of my user ID, my password and any other user authentication identification that I am required to input to access PHIMS.

4.2. I acknowledge that all actions taken in PHIMS under my user ID and password are deemed to have been taken by me, and I agree that I will be solely responsible for all activities that occur using my user ID and password. To help prevent others from accessing PHIMS using my user ID and password;

(a) I will not disclose my user ID or password to anyone else;

(b) I will not allow the computer's browser to remember my PHIMS username and password, and

(c) I will log out of PHIMS as soon as I have completed each session to prevent others from accessing PHIMS using my user ID and password.

4.3. If I suspect that my password has been obtained or used by another person, I will immediately notify the Manitoba eHealth Service Desk (by phone: (204) 940-8500 or 1-866-999-9698; by fax: (204) 940-8700; or by email: sevicedesk@sharedhealthmb.ca) and change the password. I will also immediately advise my Authorized Organization.

4.4. I am aware that my access to and my activity on PHIMS will be logged and may be monitored and audited by Manitoba Health and my Authorized Organization, on a random or as required basis and will also be audited if a breach of security is reported or suspected.

4.5. I understand and agree that Information about my access to and activity on PHIMS that is included in any audit, including Personal Information about me, may be disclosed to my Authorized Organization and shared between Manitoba Health and my Authorized Organization in the course of any audit.

4.6. I will refrain from any action which will or may disrupt the operation or availability of PHIMS or will inappropriately modify or delete the Information in PHIMS.

5. Record of user activity

5.1. I understand that PHIMS is capable of creating a record of user activity and that the individual the Information is about will be given, on request, an excerpt from the record of user activity showing a list of persons, by name, who have viewed that individual's Information in PHIMS, in accordance with the *Personal Health Information Regulation* made under PHIA.

6. Maintaining Confidentiality

6.1. I will keep confidential all the Information which I access from PHIMS and accordingly will comply with these Terms of Use, my legal obligations and my Authorized Organization's policies and procedures applicable to such Information.

6.2. When a computer screen is displaying the Information from PHIMS, I will not leave it unattended and take all reasonable efforts to ensure that no one is inappropriately viewing the screen.

6.3. I will access and use PHIMS only from computers or devices approved by my Authorized Organization. I will not download, save or store personal health information (including, but not limited to, personal health information contained in data, reports, screen shots or other documents) from PHIMS to an electronic device that has not been provided by my Authorized Organization for the purpose of using PHIMS,.

6.4. I will not download, save or otherwise transfer any Information from PHIMS onto any portable media storage device (e.g., laptop hard drive, USB drive, disk, mobile device) unless such use has been authorized by my Authorized Organization, and the device or media contains suitable encryption software. I will securely destroy any transitory Information stored on any device or media immediately upon it being no longer required for the purpose it was downloaded, saved or otherwise transferred.

6.5. I will not leave a portable media storage device (e.g. laptop hard drive, USB drive, disk, mobile device) containing PHIMS information, that has been provided by my Authorized Organization, unattended at any time, unless the device is powered down or the screen lock and password protection is activated. When not in use, I will ensure the device and any paper records containing PHIMS information is physically secured by means including in a locked desk, filing cabinet or room or has been secured by a cable lock in accordance with my Authorized Organization's security policies.

6.6. When I am in possession of Information stored on paper, a laptop or portable media storage device during transit from one location to another, I will keep the Information in my personal possession until such time that the Information can be properly secured per my Authorized Organization's security safeguards.

7. Duty to report breaches

7.1. I will report to my Authorized Organization any actual, suspected or potential privacy or security breaches involving PHIMS (whether caused by me or another person) immediately in accordance with the applicable laws, policies and procedures of my Authorized Organization and the terms of this Schedule. I understand that my Authorized Organization will ensure Manitoba Health is informed immediately either by me or my Authorized Organization for the purpose of containment, as required

under Section 14.1 of the Agreement. If I am unable to immediately notify my Authorized Organization of the actual, suspected or potential privacy or security breach, I am authorized and required to immediately notify Manitoba Health, Legislative Unit, at 204 788 6612, fax 204 945 1020, or email PHIAinfo@gov.mb.ca, and, will notify my Authorized Organization as soon as possible thereafter of this notification.

8. Ending my relationship with PHIMS

8.1. If I want to terminate my access to PHIMS, I may do so at any time by notifying my Authorized Organization or the Shared Health Service Desk.

8.2. My Authorized Organization and/or Manitoba Health, through Shared Health Inc., may also terminate my PHIMS access at any time if:

(a) I am no longer employed or engaged by my Authorized Organization;

(b) I am no longer carrying out the employment- or contract-related activities, duties or tasks that require access to PHIMS;

(c) I breach:

(i) any laws pertaining to the protection of the Information;

(ii) any provision of this Terms of Use document ;

(iii) my Authorized Organization's policies and procedures respecting access to PHIMS and the protection of the Information,

or I have acted in manner which clearly shows that I do not intend, or I am unable, to comply with my obligations under any applicable law, agreement or policy;

(d) I conduct myself in a manner that puts PHIMS and the Information in PHIMS at risk of unauthorized access, use, disclosure or retention; or

(e) Manitoba Health and my Authorizing Organization terminate the Agreement;

8.3. I understand that if my access to PHIMS has been terminated by Manitoba Health under Subsection 8.2(c) or (d) that notification may be sent by Manitoba Health to my Authorized Organization and to any applicable professional bodies. I also understand that Manitoba Health will inform my Authorized Organization in the event that such notification is sent to any applicable professional bodies.

8.4. I understand that if I breach or misuse PHIMS under Subsection 8.2(c) or (d), I may be subject to disciplinary action by my Authorized Organization, including termination of my access to PHIMS and that notification may be sent to Manitoba Health and to

any applicable professional bodies.

9. License Terms

9.1. I understand that PHIMS uses licensed software product called "Panorama" and is the property of IBM Canada Limited (the "Licensor").

9.2. I acknowledge that the Panorama software contains valuable confidential and proprietary information of the Licensor.

9.3. I understand that I will not:

(a) reverse assemble, reverse compile, or otherwise translate PHIMS unless expressly permitted by applicable law without the possibility of contractual waiver;

(b) further sublicense or transfer the sublicence for PHIMS; or

(c) sell, lease, license or otherwise distribute PHIMS to any Authorized User or any other party

10. Changes to the Terms of Use

10.1. I understand that any changes to the Terms of Use document will be brought to my attention in which case I will be asked to agree to the revised Terms of Use presented to me at that time. I further understand that if I do not agree with the revised Terms of Use, my access to PHIMS will be terminated.

11. Training

11.1. I acknowledge that Manitoba uses a Train-the-Trainer approach and my Authorized Organization's designated trainer is responsible for providing appropriate training on the use of PHIMS.

11.2. I acknowledge that it is my responsibility to ensure I have been trained on the Authorized Use of PHIMS.

12. Survival of Certain Terms of Use

12.1. I understand that even if my access to PHIMS is terminated, I must continue to comply with Sections 6.1 and 9 above.

I have read and understand this Terms of Use document, and agree to be bound by it.

Name (Printed)	Position
Signature	Date

This is Schedule "B" to the Information Sharing Agreement for Access to and Use of the Public Health Information Management System (PHIMS)

between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

SCHEDULE B – PLEDGE OF CONFIDENTIALITY

I ACKNOWLEDGE THAT I have reviewed the policies and procedures of 24-7 Intouch, Inc on the collection, use, disclosure, protection, alteration, retention and destruction of personal health information and personal information (the "Information").

I UNDERSTAND THAT I am bound by the requirements of the Terms of Use Agreement and by the policies and procedures established by 24-7 Intouch, Increspecting the collection, use, disclosure, protection, accuracy, alteration, retention and destruction of the Information.

I UNDERTAKE AND AGREE THAT:

1. I will not collect, use, disclose, alter, retain or destroy the Information except in accordance with the Terms of Use Agreement and any applicable policies and procedures of 24-7 Intouch, Inc..

2. I will treat the Information to which I have access under the Terms of Use Agreement as strictly confidential and will use the Information solely for the purposes outlined in the Terms of Use Agreement and for no other purpose.

3. I will only access Information that I am authorized to use and that I need to know to carry out my work-related duties.

4. Except when necessary to carry out my work-related duties and in accordance with the Terms of Use Agreement document:

    a. I will not retain or make copies of any Information, in any form or medium, and

    b. I will not disclose or permit access to any Information, in any form or medium, to any person, corporation, organization or entity.

I ACKNOWLEDGE THAT failure to comply with the undertakings in this Pledge of Confidentiality may result in a breach of *The Personal Health Information Act* ("PHIA") and *The Freedom of Information and Protection of Privacy Act* that can result in disciplinary action up to and including dismissal, the imposition of a fine if found guilty of an offence under PHIA and, where applicable, a report to my health profession regulatory body.

Name (Printed)

Position

Signature

Date

This is Schedule "C" to the Information Sharing Agreement for Access to and Use of the Public Health Information Management System (PHIMS)

between Manitoba and **24-7 Intouch, Inc.** **(the "Agreement")**
(insert name of Organization)

See attached.

Business Transformation and Technology

Manitoba Government

Electronic Media Disposal Standards and Procedures

Version 1.0 November 2005

Table of Contents

Introduction

Background

This document provides standards and procedures for the secure reuse and disposal of computer media containing government information. The Information Protection Centre (IPC) developed and maintains this document under the direction of Manitoba Information and Communications Technologies. The standards and procedures are necessary to ensure that confidential government information, personal, personal health, or other identifying information about third parties or businesses, cannot be retrieved from computer media accidentally or intentionally, by unauthorized persons within or outside of the Manitoba government.

This document includes standards and procedures for a number of media types. Various media types can have a significantly different standard and procedure for the safe removal of data.

Government Records

Retention and disposal of government records is governed by *The Archives and Recordkeeping Act* (ARA). Most e-mail messages, documents and other electronic records created or received in the course of government business are **government records**. This means that the records must be captured (filed) in a recordkeeping system, and retained and disposed of according to the provisions of an approved records schedule.

Government employees are responsible for ensuring that government records under their control are properly retained and disposed of.

Prior to destroying information or disposing of media containing government information, it is critical that the user (or the employee or work group responsible for the information) ensure that all information and records required for government business and recordkeeping purposes have been retained and managed in accordance with the ARA.

Employees must follow proper procedures for managing and disposing of electronic documents created or received in the desktop environment, including e-mail and other files created using desktop applications and stored in network servers, computer hard drives or removable storage media.

Government records maintained in electronic form in other types of systems are subject to the same requirements for authorized retention and disposal. This means that retention rules should be defined in advance and reflected in approved records schedules, and that provision must be made to ensure the records are maintained, protected, and accessible for as long as required – whether in native formats in the original system, or in other appropriate formats, systems or media. Responsibility for defining the retention requirements and preparing records schedules rests with the business area responsible for the records. IT specialists must ensure that all data required to support, manage and access these electronic records is retained, prior to disposing of data on computer storage media.

Disposal Standard for Hard Disk Drives

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of hard drive assets including disposal.

Hard drive assets that are to be reused elsewhere within government departments must be wiped to ensure all data is unavailable for inappropriate access.

Hard drive assets that are being disposed outside of government must be wiped or destroyed to ensure all data is unavailable for inappropriate access.

The destruction of information or disposition of hard drives containing government information must be managed in accordance with *The Archives and Recordkeeping Act.*

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE function that does not result in the secure deletion of the data stored on the hard drive; rather file and directory pointers are erased without ever touching the actual data. As a result of this process, data that is erased using the operating system DELETE/ERASE function can be easily recovered.

Many devices including, but not limited to, printers, photocopiers, and multifunction devices include hard drives. The hard drives in these devices can retain sensitive information that can be easily recovered.

Hard drives used by the Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the hard drive disposal standard and procedure.

Standard

As a general principle, all private, valuable, and confidential data should be stored on Network file servers where proper backup and recovery procedures are in place. Local workstation hard drives are not backed up as part of standard operating procedures. The following paragraphs outline the steps required to dispose of a hard drive depending on the specific circumstance.

Transfer of hard drives within a department: Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. If the hard drive is remaining within the department, the drive can be reformatted prior to transfer because special recovery tools would be required by an individual to access the data erased on the hard drive. In the event the hard drive contained sensitive information it is recommended that it be sanitized using the disk wiping procedures outlined in the procedure section of this document unless the hard drive has been encrypted using Government approved encryption software.

Disposal of hard drives to other departments or organizations outside of the Government: Prior to disposal or transfer to another department, working, usable hard drives must be overwritten in accordance with the disk wiping procedures. The owner must be able to certify that the hard drive was properly sanitized. Certification should include the make, model, and government asset tag number of the computer or stand alone hard drive and the date that the procedure was performed. Equipment designated for surplus or other disposal must have some form of identification stating that the hard drive has been properly sanitized. This could include a physical label or some form of electronic identification written to the hard drive.

Repairing a hard drive under warranty:

Hard drive manufactures and computer suppliers typically require the return of defective hard drives under warranty. Some suppliers will allow customers to declare when certain hard drives contain sensitive information by completing the required declaration forms. Drives that have been verified by the manufacturer as defective do not have to be returned to the manufacturer. The failed hard drive must then be destroyed following the procedures for hard drive disposal.

When the manufacturer requires that the failed disk drive be returned for warranty, and the hard drive is unencrypted, a risk assessment must be conducted to determine the sensitivity of the data on the hard drive. If there is potentially sensitive data on the failed hard drive then the old drive must be properly destroyed and the owner of the system must assume any costs associated with purchasing a new drive.

Hard drives can be returned for warranty repair or replacement without concern for the sensitivity of the data when the hard drive is encrypted or part of a file server configured with RAID 5 (Redundant Array of Inexpensive Disks), and the data spread across three or more disks.

Disposal of damaged or inoperable hard drives off warranty: For hard drives that are off warranty and inoperable the drives must be physically destroyed.

Return of leased equipment: Lease agreements typically require that equipment be returned intact to the leasing company. Workstation hard drives must have the data sanitized using the

disk wiping procedures. Certain devices have hard drives but cannot run the disk wiping software, including but not limited to, certain proprietary servers, printers, fax machines, or other multi function devices. For these types of devices the hard drives must be destroyed or degaussed and the owner of the device must assume any associated costs. When negotiating lease arrangements considerations must take into account the requirements of this standard.

Roles and Responsibilities

End users are responsible for erasing all personal and business data from their hard drives before return to the department.

Departments are responsible for ensuring that all hard drives are wiped before they are made available for new use within Government.

Departments are responsible for ensuring that all surplus hard drives are disposed of in accordance with the disposal standard.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

MICT is responsible for ensuring that all surplus computer equipment destined for Computers for Schools and Libraries are wiped of all sensitive information.

There must be an audit trail that shows hard drives have been wiped, degaussed, or physically destroyed at the appropriate time.

Procedure - Disposal of Hard Drives

Methods for Secure Information Disposal

There are three primary methods for secure disposal of hard drives. Total destruction and disk wiping are the two preferred methods. Hard disk degaussing is not recommended due to the high cost of hard disk degaussing equipment and the complexity of the degauss process. If degaussing equipment and trained staff are available then degaussing is an acceptable method of erasing data.

1) Total Destruction

The Manitoba Government donates surplus computer equipment to Computers for Schools and Libraries. Therefore total disk destruction is not the preferred method of disposal for hard drives in personal desktop or laptop computers.

For file servers it must decided whether the extra cost and time involved in wiping is justified. Disk erasure software is often incompatible with proprietary server hardware. Departments should consider whether the cost associated with the secure disposal will exceed the value of the asset. If it is more cost effective, then choose total destruction by an approved vendor as the primary option for server hard drives.

2) Disk Wiping (Overwriting)

Disk wiping software involves methods of writing 1's to the entire disk, followed by writing 0's on top of the previous 1's. With each pass the chance of recovery is greatly reduced. A minimum of 1 pass is required with 3 passes required for highly confidential or extremely sensitive information. Government hard disks sent to Computer for Schools and Libraries must be wiped once at source (originating location) and a second time at Computers for Schools and Libraries using Government approved disk wiping software.

3) Degaussing

Degaussing magnetically erases data from magnetic hard drives. When done properly, it renders any previous stored data unreadable. Degaussing requires the purchase of a degaussing product, frequent product testing and a skilled operator. The result of degaussing can vary depending on how it is performed. Hard disk degaussing renders the hard drive inoperable. For this reason degaussing is not recommended for drives that will be sent to Computers for Schools and Libraries. Hard disk degaussing is also not recommended because of the high costs associated procuring degaussing equipment. When degaussing equipment and skilled operation staff are available degaussing is an acceptable alternative for drives that are not going to Computers for Schools and Libraries and for hard drives that have failed or are from proprietary servers that cannot run the disk wiping software.

Disposal Standard for Magnetic Tapes

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of magnetic tapes.

All magnetic tapes that have not been degaussed must be physically destroyed when disposing of the magnetic tape media.

To prevent loss of privacy, magnetic tapes that are to be reused elsewhere within government must be carefully degaussed to remove proprietary government information.

The destruction of information or disposition of magnetic tapes containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Magnetic tape media used by the Government of Manitoba may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this material must be the primary goal of the magnetic tape disposal process.

Standard

As a basic principle, magnetic tapes must be securely degaussed each time they are used in a new application environment. For example a magnetic tape used to backup a sensitive production system must be securely degaussed before reuse within the application environment for backing up a less sensitive information system. This ensures that no residual data from the sensitive production system remains on the magnetic tape.

Degaussing of magnetic tape must be performed with a degaussing unit of sufficient field strength for the media being sanitized. Refer to the manufacturer specification for the magnetic tape degaussing unit.

Magnetic tapes must not be reused in other departments, boards, agencies, or special operating agencies without degaussing.

Magnetic tapes that have not been degaussed, and are no longer of use to back-up or store information, must be securely physically destroyed.

Roles and Responsibilities

Departments are responsible for degaussing or physically destroying of all magnetic tapes.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that magnetic tapes have been disposed of in an appropriate fashion through either degaussing or physical destruction. There must be an audit trail that shows all magnetic tape has been degaussed or physically destroyed at the appropriate time.

Procedure - Disposal of Magnetic Tape

As a minimum precaution magnetic tapes must be degaussed:

- When returned for warranty replacement
- When leaving the Government's controlled environment
- Prior to reuse in a new application environment
- Prior to reuse in other Government Departments, or
- When going to disposal without physical destruction.

In environments where no degaussing equipment exists, or when the tapes contained highly sensitive information, the magnetic tapes must be physically destroyed prior to disposal. Shredding is the preferred method for destroying magnetic tape media.

Commercial shredding operations offer mobile shredding services. Tapes destroyed using mobile shredding services do not require degaussing prior to destruction provided the shredding operation is monitored and validated by Government staff.

Physical destruction of media via incineration is typically not recommended. Although this may be effective physical destruction method safety, environmental and/or health concerns preclude using such procedures.

Disposal Standard for Optical (CD/DVD) Media

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of optical media. For the purpose of this document optical media includes, but is not limited to, read only and rewriteable compact disks (CD) and digital video/versatile disks (DVD).

Optical media has no secure erase capability; as a result, secure disposal, destruction, is the only viable option for this media type.

The destruction of information or disposition of optical media containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Optical media used by the Government of Manitoba may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the optical media disposal standard and procedure.

Standard

When the optical media is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed.

When optical media is used to dispense licensed software, physical destruction of the media should occur in conjunction with the expiration of the software license.

If the media content is particularly sensitive, shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical.

Roles and Responsibilities

Departments are responsible for physical destruction of all optical media.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that optical media has been disposed of in an appropriate fashion. There must be an audit trail that shows all optical media has been physically destroyed at the appropriate time.

Procedure - Disposal of Optical Media

When the CD or DVD storage media is no longer of use it must be physically destroyed.

Methods for Secure Information Disposal

Shredding is the preferred disposal method for optical media.

Multiple shredding passes are not normally recommended as this can create excessive plastic dust which is not appropriate in an office environment.

Physical destruction of media via sanding, or incineration, is typically not recommended. Although these may be effective physical destruction methods, safety, environmental and/or health concerns preclude using such procedures.

Government departments should consider the use of commercial shredding operations to safely destroy their optical storage media when appropriate shredding equipment is not available within the department.

Disposal Standard for Diskettes

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of diskettes including disposal. For the purpose of this document the term diskette refers to soft, or flexible, media types such as floppies and Zip disks and does not include CD or DVD media.

Before disposal all Diskettes must be carefully cleansed of proprietary government information to guard against inappropriate access. To prevent loss of privacy, media that are to be reused elsewhere within government must have data securely erased.

The destruction of information or disposition of diskettes containing government information must be managed in accordance with *The Archives and Recordkeeping Act*.

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE or Format function that does not result in the secure deletion of the data stored on the diskette; rather file and directory pointers are erased without ever touching the actual data. Data that is erased using the operating system DELETE/ERASE or Format function can be easily recovered.

Diskettes used by the Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the diskette disposal standard and procedure.

Standard

When diskette media is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed or securely erased using wiping software.

When diskette media is used to dispense licensed software, physical destruction of the media should occur in conjunction with the expiration of the software license.

If the media content is particularly sensitive, shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical

Roles and Responsibilities

Departments are responsible for physical destruction or secure wiping of all diskette media.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that diskette media has been disposed of in an appropriate fashion. There must be an audit trail that shows all diskette media has been physically destroyed, degaussed, or wiped at the appropriate time.

Procedure - Disposal of Diskettes

Methods for Secure Disposal

There are three primary methods for secure disposal of diskettes. Total destruction and degaussing are the two preferred methods. Secure erasure through wiping is a viable alternative but requires the purchase of wiping software.

Given the low cost of floppy diskettes the cost of wiping sensitive data from a diskette may not be justified. Degaussing or physical destruction of the diskette are both considered viable alternatives and recommended.

Other physical media such as ZIP Disks are more expensive than diskettes. However the cost of acquiring and using a wipe utility for ZIP cartridges may be cost prohibitive. Either degaussing or physical destruction through shredding are viable alternatives and recommended.

As a basic principle, all diskettes must be wiped each time they are to be employed by a new user. Given the cost and complexity of wiping diskette media care must be taken when sharing such media. Given the low cost of floppy media departments should consider using new media any time they are required to share data with a third party to prevent the accidental release of sensitive information.

Physical destruction of diskette media via drilling holes in the diskette, sanding, incineration, etc. is typically not recommended. Although these may be effective physical destruction methods, safety, environmental and/or health concerns preclude using such procedures. The only effective and safe method would be degaussing, or shredding of the media.

Government departments should consider the use of commercial shredding operations to safely destroy floppy diskettes or other removal storage media.

Disposal Standard for USB Memory Storage Devices

Summary

This standard and operating procedure is designed to prevent the loss of data privacy or confidentiality throughout the life cycle of universal serial bus (USB) memory storage devices including disposal. For the purpose of this document the term USB memory storage device refers to any form of storage device that plugs into a USB port and uses non volatile memory to store data.

Before disposal all USB memory storage devices must be carefully cleansed of proprietary government information to guard against inappropriate access. To prevent loss of privacy all USB memory storage devices that are to be reused elsewhere within government must have data securely erased using wiping software.

The destruction of information or disposition of memory sticks containing government information must be managed in accordance with *The Archives and Recordkeeping Act.*

Scope

This standard and the accompanying operating procedure applies to all Manitoba Government departments, agencies, boards, and commissions connected to the Manitoba Government network.

Introduction

Most operating systems have some form of DELETE/ERASE or Format function that does not result in the secure deletion of the data stored on the memory stick; rather file and directory pointers are erased without ever touching the actual data. Data that is erased using the operating system DELETE/ERASE or Format function can be easily recovered.

USB memory storage devices used within Government may contain private or confidential information that must not be shared in a public forum. This information may occur in several forms, the most common being:

- Personal, or Personal Health information about citizens of the province of Manitoba
- Confidential business information
- Confidential information about provincial employees, provincial contracts and purchases, or Cabinet Confidential documents
- IT software configuration and technical support information. This information must remain confidential because of its potential to facilitate the entry of would-be intruders into Provincial networks.

Protection of this information must be the primary goal of the USB memory storage device disposal standard and procedure.

Standard

When a USB memory storage device is no longer of use to back-up or store sensitive information, the media must be securely, physically destroyed or erased using wiping software.

USB memory storage devices must be securely erased prior to reuse in other departments, boards, agencies, or special operating agencies using wiping software.

If the media content is particularly sensitive, destruction through shredding must occur to a fine enough granularities to make forensic analysis in a laboratory impractical

Roles and Responsibilities

Departments are responsible for physical destruction or wiping of all USB memory storage devices.

Departments are responsible for ensuring that all vendors and ICT outsourcing organizations comply with the disposal standard.

Departments are responsible for confirming that USB memory storage media has been disposed of in an appropriate fashion. There must be an audit trail that shows all USB memory storage devices have been physically destroyed or wiped at the appropriate time.

Procedure - Disposal of USB Memory Storage Devices

Methods for Secure Disposal

There are two primary methods for secure disposal of information on USB memory storage devices, total destruction, and secure erasure through wiping. Secure erasure using wiping software may not be practical due to the cost of procuring wiping software capable of securely erasing the USB memory storage device.

As a basic principle, all USB memory storage devices should be wiped each time they are to be employed by a new user. Given the cost and complexity of wiping USB memory storage devices care must be taken when sharing such media with third parties. Departments should consider using alternative forms of electronic media such as CD or DVD media any time they are required to share data with a third party to prevent the accidental release of sensitive information.

Government departments should consider the use of commercial shredding operations to safely destroy USB memory storage devices that are no longer of use.

Appendix A
Sample Electronic Media Clearing Standards (RCMP)

The following are the RCMP standards for secure disposal of different media types.

Hard-Disk Drives/Diskette

Protected A/B/Confidential:

a) Run thru disintegrator/pulverizer to a maximum 7.5 cm./3-inch size or (incineration) or
b) (Internal reuse) One time software overwrite
(External reuse or disposal) Three time software overwrite

Protected C/Secret:

a) (Degauss or 3-time overwrite or pre-encrypt) and run thru a disintegrator/pulverizer to a maximum 7.5 cm./3-inch size or
b) Disintegrate to 6mm/¼ inch screen size or
c) incineration

Top Secret:

(Degauss or 3-time overwrite or pre-encrypt) and run thru a disintegrator to a maximum 3mm (1/8 inch size)

Optical Media (CD's, DVD's etc)

Protected A/B/Confidential:
Surface grinding or 1.5 cm (1/2 inch) maximum size residue Protected "C"/Top Secret/Secret: Surface grinding or 3X3 mm (1/8" X 1/8") particles (disintegration) or incineration

Integrated Circuit/Flash Memory

Includes: USB Memory sticks, RAM and "Flash ROM Memory" are non-volatile

Protected A/B/Confidential

One time overwrite or damage with hammer/pulverizer/heat/incineration

Protected C/Top Secret/Secret

Highly sensitive information should not be stored on these devices but in the special case that it was, contact RCMP or CSE for instructions

Tape Media

Protected A/B/Confidential:
1.5X 1.5 cm (½" X ½") particles (disintegration) or degaussing/incineration

Protected "C"/Top Secret/Secret:

3X3 mm (1/8" X 1/8") particles (disintegration) or degaussing/incineration

Appendix B
Definitions

Destruction – To alter the physical structure of the media so that the risk of unauthorized information disclosure is minimal. Physical destruction of media should be conducted by a commercial shredding operation.

Degaussing – An electronic purging procedure. Degaussing applies a reverse magnetic field to electronic media. This changes the magnetic lines of flux and reduces the magnetic induction to zero thus eliminating information from the electronic media.

Disposal – The release or transfer of magnetic storage media outside the control of the Government.

Multifunction Device – A multi function device is an electronic device that combines the functionality of multiple computer or electronic devices such as fax, photo copier, and printer into a single device.

Reuse - To redistribute and reassign storage media and its control to different environments

Sanitization - Generic term for removing sensitive information from storage media.

Secure Erase - To erase data using wiping techniques to eliminate data from the magnetic media. A secure erase can be used to erase a file, or to erase files that were not previously erased using a secure erase process.

Shredding – A means of destroying media by mechanically cutting the media into narrow strips.

Wiping - A standard overwrite technique used to erase sensitive data from a storage media. Wiping involves methods of writing 1's to the media, followed by writing 0's on top of the previous 1's. With each pass the chance of recovery is greatly reduced.

This is Schedule "D" to the Information Sharing Agreement for Access to and Use of the Public Health Information Management System (PHIMS)

between Manitoba and 24-7 Intouch, Inc. **(the "Agreement")**

(insert name of Organization)

Schedule "D"
System Services and Related Services

1. Definitions

1.1. Capitalized terms in this Schedule D, unless otherwise defined below, will have the meanings set out in subsection 2.1 of the Agreement. The following additional terms have the following definitions for the purposes of this Schedule D:

(a) "Authorized Sponsor " means a designated representative of the Organization who has the authority to determine who needs access to PHIMS in order to perform his/her employment / contractual duties. The Authorized Sponsor designates Authorized Users and assigns User Role.

(b) "Authorized Account Requestor" means a designated representative of the Organization who assists the Authorized Sponsor in submitting approved account requests to the Shared Health Service Desk and will be a contact to forward information to, or receive information from, Shared Health Health Inc. for the purpose of Authorized User account management (i.e. assigning User Role(s), adding, changing or deleting Authorized Users access to PHIMS).

(c) "Incident" means an unplanned interruption to an information and communication technology ("ICT") service or a reduction in the quality of an ICT Service;

(d) "Key Contact(s)" means a lead contact person and/or identified contact persons for points of escalation;

(e) "Service Request" means a request for information, or advice, or for a standard change or for access to an ICT service or a request for the performance of services by the Information Manager, Shared Health Inc. such as requesting new user accounts or a configuration change to an application.

2. Service Description

2.1. PHIMS is an integrated, electronic public health record that improves and supports the delivery of population-level preventive interventions including, but not limited to, the surveillance and management of communicable disease cases and outbreaks, immunizations and vaccine inventory management. It also provides work management and notifications to support these functions.

2.2. The PHIMS Shared Service means the following software and services:

(a) License to use the most current release of the software system called "Panorama" in accordance with the License grant set out in Section 3.0, including:

(i) The PHIMS modules for immunization, inventory, investigation, outbreaks, family health, indexes, business shared services and reports;

(ii) The viewable, printable and searchable computer application and technical support services that provide Authorized Users with secure real-time access to Information in the PHIMS Database; and

(iii) all releases, hot fixes, enhancements, modifications and improvements to the PHIMS made from time to time;

(b) Support for the following PHIMS interfaces: the Provincial Client Registry System, Physician Billing (CPS), The Drug Program Information Network (DPIN) and the Canadian Blood Services (CBS) Rh Trace Line when it is implemented, and Cadham Provincial Lab results when implemented; and

(c) Shared Health Service Desk Services as described in Section 8.

3. Licensing

3.1. Subject to the subsections in this Section 3, Shared Health Inc. (formerly eHealth) grants to the Organization a nonexclusive, perpetual, paid-up, royalty-free sublicense to access use, execute, and display the PHIMS (including the software products called "Panorama") and select functionalities (including all updates and enhancements of the same), for the purpose set out in the Agreement, in accordance with the following:

(a) Subject to clauses (b) to (e) below, this sublicense is for internal use only and does not permit the Organization or its respective Authorized Users to sublicense to others;

(b) The Panorama software is deemed to be Confidential Information of IBM Canada Limited ;

(c) The Organization agrees not to:

(i) reverse assemble, reverse compile, or otherwise translate PHIMS unless expressly permitted by applicable law without the possibility of contractual waiver;

(ii) further sublicense or transfer the sublicence for PHIMS; or

(iii) sell, lease, license or otherwise distribute PHIMS to any Authorized User or any other party;

(d) This sublicense includes the right to have the Organization's employees and contractors acting on its behalf to do any of the foregoing (which shall include use by outsourcers solely in support of, or as required by, systems on which PHIMS is operated). Without limiting the generality of the foregoing this right includes any third party persons contracted to implement and/or support the PHIMS System;

(e) This sublicense includes the right for the Organization to have Authorized Users use PHIMS for the authorized purposes set out in Section 3.2 of the Agreement within Manitoba, and from outside Manitoba as required for the purpose of the Agreement, in accordance with the terms of this Schedule.

4. Shared Health Inc.'s Responsibilities

4.1. Shared Health Inc. will:

(a) provide the PHIMS Shared Service as described in Subsection 2.2 to the Organization during the Term of the Agreement;

(b) provide the PHIMS Shared Services in accordance with its service commitment guidelines, which are available on request;

(c) work with the Organization's Key Contacts, if required, to develop an appropriate support model;

(d) maintain technical currency of its assets used in the delivery of its hosting service except where the PHIMS-Panorama vendor recommends specific versions of supporting software or infrastructure in order to ensure compatibility and Shared Health Inc. is not able to implement such software within its current budget or financial constraints;

(e) notify the Organization of the technical requirements to ensure compatibility of the Organization's ICT components that access, interface, and support the PHIMS (including, but not limited to, networks, source systems, workstations and peripherals) with the PHIMS Shared Service software and infrastructure;

(f) email outage notifications to the Key Contact person(s) identified by the Organization;

(g) provide, at minimum, seven (7) days of advance notice to the Organization for planned outages;

(h) provide as much notice to the Organization as possible for unplanned outages;

(i) provide the Organization with its Service Desk Description Document as may be amended from time to time, which document is primarily for Shared Health Inc. managed laptops and works stations.

5. The Organization's Responsibilities

5.1. The Organization will:

(a) satisfy or cause its Authorized Users to satisfy all pre-requisites as identified in Section 7 of this Schedule;

(b) access support through Shared Health Inc.'s Service Desk Service as required to address Incidents and Service Requests related to the PHIMS Shared Service;

(c) provide and maintain support of its ICT components that access, interface, and support the PHIMS Shared Service including, but not limited to, networks, source systems, workstations and peripherals;

(d) provide to Shared Health Inc.'s, and update regularly, a list of its employees designated as Authorized Sponsor and Authorized Account Requestors;

(e) have a standard support model to provide guidance to the Shared Health Service Desk with respect to points of escalation;

(f) provide to Shared Health Inc. the contact information for its Key Contacts;

(g) provide contact information of Key Contacts who should be contacted for service outage notifications;

(h) provide Shared Health Inc. troubleshooting and support model information, if the Organization is adding services that require Shared Health Service Desk support (e.g. an interface between PHIMS and the Organization's unique requirements);

(i) maintain technical currency, where possible, of its ICT components as advised by Shared Health Inc.;

(j) be responsible for developing and executing procedures required to continue with clinical and business workflows in the event of any outages to ensure it is able to continue with its services notwithstanding the unavailability of the PHIMS Shared Service;

(k) follow the provisions of the Agreement as they apply to the Organization.

6. Authorized Users

6.1. Authorized Users must be authorized by an Authorized Sponsor and/or Authorized Account Requestor in accordance with the requirements of Section 7 of the Agreement.

6.2. For security purposes, a request for a PHIMS account for a new Authorized User must be made only by an Authorized Account Requestor.

6.3. Authorized Account Requestors must request new accounts for Authorized Users using an Account Service Request form, as required by Manitoba and Shared Health Inc.

7. Prerequisites

7.1. The Organization and its Authorized Users must meet the following prerequisites for the PHIMS Shared Service:

(a) The Organization must satisfy the technical requirements posted on the PHIMS website;

(b) will only access and use PHIMS from secure electronic devices which are provided by the Organization unless there has been prior written approval from MHSAL. where an Authorized User will be storing Personal Health Information or Confidential Information downloaded from PHIMS onto a designated electronic device, or uploaded to PHIMS from their device, or through storage of reports on their device, the device must contain suitable encryption software and password protection; and

(c) each Authorized User must agree to the Terms of Use as identified in Section 8.3 of the Agreement.

8. Shared Health Service Desk Services

8.1. Shared Health Inc. will provide call support to Authorized Users of the PHIMS Shared Service, in respect of clinical, technical and system access requests, as follows:

(a) The Organization will designate "Super Users" (also known as peer supporters), who must be Authorized Users, as the preferred first point of contact for troubleshooting PHIMS issues for Authorized Users. If the Super Users cannot assist the Authorized User or if the Super User is unavailable, the Authorized User may call Service Desk directly;

(b) the Service Desk call support will be available as set out in the Service Desk Description Document as referred to in 4.1(i) and in Section 9 of this Schedule on a 24/7 basis for Level 1 Incidents and Service Requests, and for technical support Incidents and Service Requests that are Priority 1 and 2;

(c) the Service Desk will provide the initial assessment and will either resolve at first contact or triage to the appropriate technical support area within Shared Health Inc.;

(d) Incidents will be tracked by priority in relation to patient care and business criticality;

(e) Shared Health Inc. will use its standard ticketing process and assign a priority level to Service Desk requests, in accordance with its guidelines or standards for assigning priorities to Service Desk tickets;

(f) the standard Service Desk service provides:

(i) instructions and support on the use and functionality of standard desktop hardware and software applications (for Authorized Users with Shared Health Inc. provided workstations) information gathering, analysis, and troubleshooting;

(ii) initial assessment, prioritization, and logging of Incidents and Service Requests;

(iii) access, coordination and communications in accordance with Shared Health Inc.'s service practises, including account management, change management, incident management, problem management, and release management;

(iv) resolution of common Incidents or Service Requests, such as those pertaining to:

(a) system access, including PHIMS password resets;

(b) general desktop hardware and software issues (for workstations not managed by Manitoba eHealth, referral back to the Organization's IT support may be required in some cases);

(v) routing of Incidents and Service Requests that cannot be resolved at the Service Desk to Level 2 (L2) support groups, including to the Organization's support structures as appropriate;

(vi) follow-up and quality assurance activities as required to resolve and close Incidents and Service Requests.

8.2. To engage the Shared Health Service Desk, the Organization or its Authorized Users will send requests to Shared Health Service Desk via email or phone as follows:

Service Desk contact information:
Phone: 204-940-8500
Toll Free: 1-866-999-9698
e-mail: Servicedesk@sharedhealthmb.ca

8.3. When contacting the Shared Health Service Desk, the Authorized User must provide the following information:

(a) full name;

(b) contact information;

(c) site/current location; and

(d) nature/purpose of their call; and as much relevant information as possible relating to the Incident.

8.4. Authorized Users must be prepared to respond to the authorization/validation questions from Shared Health Service Desk personnel.

9. Hours of Service by Shared Health Service Desk

9.1. Hours of Service are as follows:

Hours of Operation	24/7 Monday to Friday; statutory holidays excluded
Scheduled Maintenance	☒ Yes PHIMS Scheduled maintenance is performed Wednesdays 18:00-06:00 No
Support Hours - Service Requests and Incident Reporting	
Level 1 Incidents and Service Requests[1]	24/7
Level 2 Incidents and Service Requests[2]	☒ Monday to Friday 0830-1630 CST; statutory holidays excluded

1 Level 1 support is primarily for Incidents and Service Requests involved with Manitoba eHealth managed laptops and workstations, unless for PHIMS password re-sets.

2 Level 2 support is for any work required from the PHIMS (Panorama) Operations Support team: PHIMS (Panorama) Clinical Analysts, PHIMS (Panorama) Application Administrators, or PHIMS (Panorama) Application Support Analysts.

This is Schedule "E" to the Information Sharing Agreement for Access to and Use of the Public Health Information Management System (PHIMS)

between Manitoba and 24-7 Intouch, Inc. (the "Agreement")

(insert name of Organization)

SCHEDULE E CERTIFICATE OF DESTRUCTION OF INFORMATION

In accordance with subsection 14.4 of the Agreement, I _____ (Name and Position), certify the following:

1. On_____(Date), I destroyed all forms of the following Information, or I directed the destruction of the following information and I reasonably believe it will be destroyed, including all known copies, including back up copies and copies stored on computer hard drives or other portable media storage devices:

2. I have destroyed the Information, or I have directed the destruction of the Information and I reasonably believe it will be destroyed, in a manner that adequately protects the confidentiality of the Information and which is appropriate to the medium in which the Information was recorded, in a manner that makes it impossible to read or reconstruct the Information and in accordance with Schedule "C" of the Agreement and in accordance with applicable legislation. In particular, the following method of destruction was used:

Certified by: _____ _____

Officer's signature Position

Date: