CANADIAN PARTNERSHIP AGAINST CANCER | PARTENARIAT CANADIEN CONTRE LE CANCER

REQUEST FOR PROPOSALS

For IT Support Services – Service Desk, Application Management & Managed Hosting

RFP No. RP 220-2016-03

RFP ISSUE DATE	Monday, September 12, 2016
1 UNIVERSITY AVE. OFFICE SITE VISIT	Friday, September 30, 2016 from 12:00:00 to 1:00:00 p.m. local Toronto time
INFORMATION SESSION	Friday, September 30, 2016, from 1:00:00 to 3:00:00 p.m. local Toronto time
DEADLINE FOR PROPONENT ENQUIRIES	Thursday, October 6, 2016 no later than 3:00:00 p.m. local Toronto time
DEADLINE FOR ISSUING ADDENDA & RESPONSES TO PROPONENT ENQUIRIES	Tuesday, October 11, 2016 by 4:00:00 p.m. local Toronto time
PROPOSAL SUBMISSION DEADLINE	Thursday, October 20, 2016 no later than 3:00:00 p.m. local Toronto time
PROPONENT INTERVIEWS	Week of November 7, 2016

PROPONENT ENQUIRIES only by e-mail to: procurement@partnershipagainstcancer.ca

**** Proponents should reference this RFP number (RFP No. RP 220-2016-03) in the subject line of their correspondence.****

TO BE CLEAR, AND NOTWITHSTANDING ANY OTHER TERM OF THIS REQUEST FOR PROPOSALS THAT MAY BE INTERPRETED OTHERWISE, IT IS NOT THE INTENT OF THE PARTNERSHIP, NOR THE EFFECT OF THIS RFP, TO INITIATE CONTRACTUAL RELATIONS BY THE PROVISION OF A PROPOSAL BY ANY PROPONENT IN RESPONSE TO THIS RFP.

NOTWITHSTANDING ANY OTHER TERM OF THIS RFP, THIS RFP IS MERELY A CALL FOR PROPOSALS AND NOT A TENDER CALL INTENDING TO PLACE LEGALLY BINDING OBLIGATIONS ON THE PARTNERSHIP OR ON ANY PROPONENT TO ENTER INTO AN AGREEMENT OR TO BE BOUND BY ANY OF THE TERMS OF ITS PROPOSAL. IT IS NOT THE INTENTION OF THE PARTNERSHIP TO ENTER INTO AN AGREEMENT FOR THE IT SOLUTION DESCRIBED IN THIS RFP OR ENTER INTO ANY OTHER LEGALLY BINDING OBLIGATIONS UNLESS AND UNTIL THE PARTNERSHIP HAS COMPLETED THE NEGOTIATION AND FINALIZATION OF AN AGREEMENT SATISFACTORY TO BOTH THE PARTNERSHIP AND THE PROPONENT, IF ANY, THAT THE PARTNERSHIP DETERMINES TO NEGOTIATE WITH.

IT IS CONCEIVABLE THAT THESE EVENTS WILL NOT OCCUR DUE TO THE DISCRETION OF THE PARTNERSHIP AND/OR ANY PROPONENT TO NOT PROCEED, AS THERE IS NO LEGALLY BINDING OBLIGATION ON THE PARTNERSHIP OR ANY PROPONENT TO PROCEED.

DISCLAIMER

The Canadian Partnership Against Cancer Corporation disclaims responsibility for all warranties and conditions with regard to electronic files and any contents thereof. The Partnership makes no guarantee or representation that electronic files are error-free, nor compatible with recipient's systems, nor free from viruses. The Partnership will not be held responsible for any problems or injuries that arise including, but not limited to, the reliability or safety, of the use of its electronic files, in whole or in part.

History of the Partnership

The Canadian Partnership Against Cancer (the Partnership) works with Canada's cancer community to reduce the burden of cancer through co-ordinated system-level change. Grounded in and informed by the experiences of those most affected by cancer, the organization plays a unique role working with partners to support multi-jurisdictional uptake of the knowledge emerging from cancer research and best practices in order to optimize cancer control planning and drive improvements in quality of practice across the country. Partners include provincial and territorial cancer programs; federal organizations and agencies; First Nations, Inuit and Métis organizations; national health and patient organizations; and individual experts who provide strategic cancer control insight and advice from both patient and professional perspectives.

Through sustained effort and a focus on the full cancer continuum from prevention and treatment through to survivorship and end-of-life care, the Partnership supports the collective work of the broader cancer control community in achieving long-term outcomes that will have a direct impact on the health of Canadians: reduced incidence of cancer, less likelihood of Canadians dying from cancer, and an enhanced quality of life of those affected by cancer. For more information, visit partnershipagainstcancer.ca. The Partnership is also the driving force behind cancerview.ca, which connects Canadians to cancer control services, information and resources. The Partnership is funded by Health Canada.

Table of Contents

OVERVIEW OF THE REQUEST FOR PROPOSALS

RFP Structure

The following is an overview of the structure of the IT Support Services – Service Desk, Application Management & Managed Hosting Request for Proposals (**"RFP"**):

Section 1: Introduction and Project Purpose and Scope – This section provides a brief introduction to Canadian Partnership Against Cancer and related background information, as well as outlines the purpose and scope of this RFP.

Section 2: RFP Scope of Work and the IT Solution – This section provides an overview of the deliverables associated with this RFP that encompasses the "IT Solution".

Section 3: Submission Requirements – This section describes the submission requirements of this RFP.

Section 4: Terms and Conditions of the RFP Process – This section describes the terms and conditions of the RFP Process including reserved rights of the Partnership and the selected Proponent.

Section 5: Evaluation Process and Criteria – This section describes the evaluation process for the IT Solution which will be used to determine the selected Proponent.

Section 6: Supplementary Terms and Conditions – This section describes the supplementary terms and conditions with respect to this RFP.

Section 7: Execution of Agreement, Notification and Debriefing – This section describes the execution of Agreement, notification and debriefing process with respect to this RFP.

List of Appendices

Appendix A	Term Sheet Compliance
Appendix B	Form of Offer
Appendix C	Rate Bid Form
Appendix D	Client Reference Form

List of Exhibits

Exhibit A	Current & Future State Information
Exhibit B	Project Work Requirements

Exhibit C	Service Desk Requirements
Exhibit D	Application Management Requirements
Exhibit E	Managed Hosting Requirements
Exhibit F	Service Level Objective Requirements
Exhibit G	Terms and Conditions of the Agreement

1. Introduction and Project Purpose and Scope

1.1 Introduction

The Canadian Partnership Against Cancer (the **"Partnership"**) works with Canada's cancer community to reduce the burden of cancer through co-ordinated system-level change. Grounded in and informed by the experiences of those most affected by cancer, the Partnership plays a unique role working with partners to support multi-jurisdictional uptake of the knowledge emerging from cancer research and best practices in order to optimize cancer control planning and drive improvements in quality of practice across the country. (See History of the Partnership).

1.2 Background

The Partnership is in its fourth year of a second five year mandate (2012-2017), and is focused on the implementation of initiatives identified across the priority areas of cancer control. The Partnership's mandate has been renewed by Health Canada with ongoing funding. The Partnership has developed a five year Strategic Plan to inform the work completed over the next five years (2017–2022). As the Partnership plans for the future, it is critically important to ensure that the right resources, processes and services are in place to support its existing and future information technology infrastructure and applications.

The Partnership's Information Technology & Information Systems (IT/IS) environment and operations have matured over its second mandate as outlined in the next section. The Partnership requires a Proponent that has the resource depth and maturity to effectively support its dynamic and demanding IT/IS environment in the third mandate (further details provided below).

IT/IS Evolution over the Partnership's Second Mandate (2012-2017)

Over the course the second mandate, the Partnership's IT landscape has evolved in a number of significant ways. Most of these changes have positioned the Partnership to be able to take advantage of the rapidly emerging cloud computing trend – Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) – that is dramatically changing the context of IT services delivery.

The notable changes that have transformed the Partnership's IT environments include:

A. *Replacement of the Oracle Webcenter stack with more responsive and agile technologies such as Igloo Software and WordPress*. The outcomes of this initiative include the ability for Partnership staff to quickly and easily author and publish content in accordance with its Digital Strategy initiatives. It also signals the advent of a "SaaS first" application delivery strategy which dramatically reduces the need for on-premise infrastructure with its associated capital costs and complexity.

B. *Introduction of Single Sign On capabilities for end users*; this has simplified end users' interaction with business applications and tools.

C. *Introduction of disciplined processes for privacy & security management and disaster recovery (DR)*. An overview of the Partnership's Privacy and Security Framework is outlined in **Exhibit A**. These processes have reduced the overall risk profile for IT service delivery across the spectrum of managed hosting, application management and end user computing.

D. *Introduction of a Records Management Program for the organization, storage and protection of corporate records*.

E. I*ntroduction of a Work from Home (WFH) Program to provide better work life balance for Partnership employees*. There are approximately 45 employees enrolled in the WFH program and provisioned with remote office equipmen.

F. *Virtualization of all server workloads using VMWare and NetApp technologies on a Cisco UCS platform*

G. *Introduction of a secondary data centre to support Disaster Recovery and Business Continuity using VMWare vCenter SRM, Exchange DAG and Active Directory replication technologies*

More recently, the Partnership has started working on;

A. Introducing an Information Technology & Information Management (IT/IM) Risk Based Auditing Plan that outlines annual areas of focus in IT/IM operations that require an increased level of attention.

B. Introducing a Business Continuity Plan for the organization.

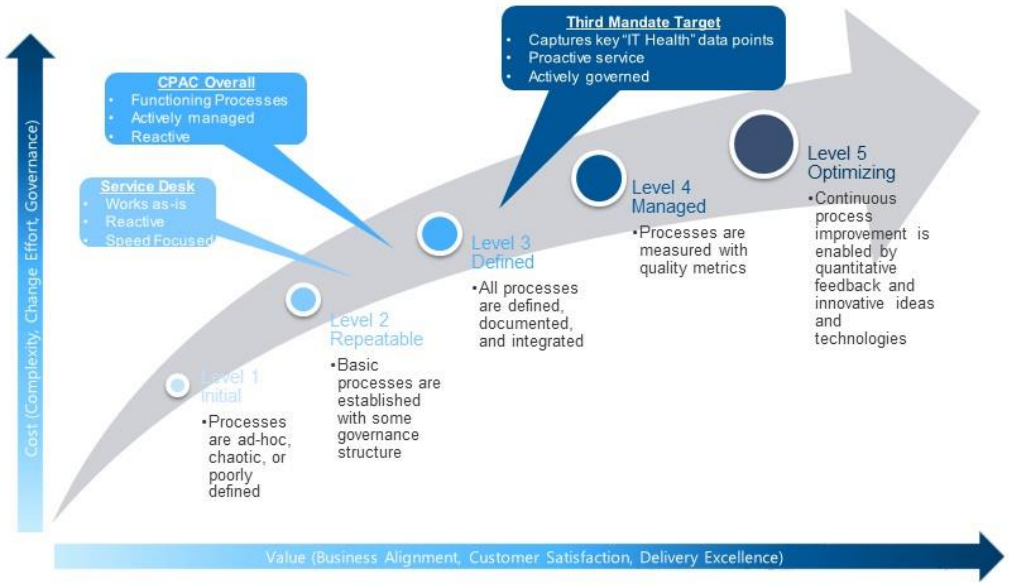
C. Introducing a revised IT Education and Training Program focused on delivering practical use-case, hands-on walkthrough style training instead of a classroom style approach which has proven to be ineffective over the second mandate.

A number of IT pilot projects are planned for this fall (September 2017 – December 2017), that will inform the transition project work (January 2017 – March 2017) and the operational support service over the contract period. Work may include;

i. Microsoft Azure Cloud Setup
ii. Office 365 and Skype for Business
iii. Window 10
iv. Meraki Z1 VPN appliance to support the Work-from-Home Program
v. IP Telephony SaaS Solution
vi. Network infrastructure upgrades at 1 University Avenue Office – WiFi & network closets

IT/IM Focus over Third Mandate

The Partnership recently completed an external assessment of its Service Desk and overall state of IT operations. The current maturity of the Partnership's IT operations and its Third Mandate target are indicated in the IT Service Management Maturity Model diagram below.



Recommendations from the external assessment will help inform key IT operational themes and areas of focus over the Partnership's third mandate. **The Proponent should clearly demonstrate in their Proposal how they will assist the Partnership to achieve successful outcomes in the following areas;**

- Service Desk Operations, Reporting & Communicatons
- IT Training and Education
- IM/IT Risk-Based Auditing
- Cloud Service Transition and Adoption

Current IT Support Contract

The Partnership's current IT Support contract ends on March 31, 2017. The current vendor will not be bidding on the 2017-2022 contract.

Current State and Future State Information

Information pertaining to the Partnership's current state of IT support and operations and future state information can be found in **Exhibit A**.

1.3 Invitation to Proponents

This Request for Proposals (the "**RFP**") is an invitation to suppliers/vendors (the **"Proponents"**) to submit proposals (the **"Proposals"**) for the provision of, among other things, the transition and implementation of IT Support Services including Service Desk, Application Management and Managed Hosting (collectively, the **"IT Solution"**, as further described in this RFP). A high level description of the contemplated IT Solution is described in Section 2, "RFP Scope of Work and the IT Solution".

This RFP is issued by the Partnership, a not-for-profit corporation funded by Health Canada.

1.4 Enquiries

Proponents should forward all enquiries and other communications, via e-mail only to: procurement@partnershipagainstcancer.ca

All enquiries should be made via e-mail to the e-mail address above and enquiries submitted in any other way will not be accepted or answered. Proponents acknowledge that all enquiries received from Proponents and corresponding responses provided by the Partnership will be disclosed to all Proponents by way of an Addendum.

All enquiries and communications should be received prior to the Deadline for Proponent Enquiries set out in Section 4.1.

1.5 Type of Agreement

It is expected that the Partnership and the contracted Proponent, if any, will negotiate and execute a comprehensive form of agreement setting out the terms and conditions that will apply to the provision of the IT Solution under this RFP (the **"Agreement"**). At the Partnership's election, it is expected that the Partnership and the contracted Proponent will first execute a form of Letter of Agreement-Term Sheet (the **"LOA-TS"**) based on the terms set out in Appendix A as a condition to the negotiation of the Agreement. Each Proponent should state in their Proposal whether they agree to the concept of a LOA-TS and to each of the terms of the Term Sheet being incorporated into the Agreement using Appendix "A", "Term Sheet Compliance". If the answer is not an unqualified yes, then a clear and specific alternative should be provided. Expressions such as but not limited to "have negotiated these concepts in the past with other customers to our mutual satisfaction", "read and understood" or "subject to review/further review by our legal counsel" will not be considered as being clear and specific alternatives.

To facilitate negotiations, the Agreement could be based on an amended form of the contracted Proponent's standard legal documentation, as amended to reflect the agreed-to terms of the LOA-TS.

Each Proponent is requested to include in their Proposal, in unlocked Microsoft Word format, an agreement or agreements that they wish to have the Partnership consider for negotiation

purposes of the Agreement. The Partnership will consider whether the form of those agreements is appropriate for the basis of negotiations.

It is the Partnership's intention to enter into the Agreement with only one (1) legal entity, (the "**Prime Contractor**"). The term of the Agreement will be for five (5) years with an option in favour of the Partnership to extend the Agreement on the same terms and conditions for two (2) additional term(s) of one (1) year each. It is anticipated that the Agreement will be executed early spring of 2017 and go-live of all operational services to occur on April 1, 2017.

For clarity, it is the intention of the Partnership to enter into an Agreement with the Prime Contractor for an overall IT Solution.

1.6 No Guarantee of Volume of Work or Exclusivity of Agreement

The Partnership makes no guarantee of the value or volume of work to be assigned to any Proponent. The Agreement executed with a selected Proponent will not be an exclusive contract for the provision of the described services and deliverables for the IT Solution. The Partnership may contract with others for the same or similar services and deliverables to those described in this RFP or may obtain the same or similar services and deliverables internally.

1.7 Trade Agreements

Proponents should note that procurements falling within the scope of the following instruments:

i. Chapter 5 of the Agreement on Internal Trade ("AIT");
ii. the Trade and Corporation Agreement between Ontario and Quebec ("Ontario/Quebec"); and or
iii. the Agreement between the Government of Canada and the Government of the United States of America on Government Procurement ("GPA")

are as applicable and subject to the terms of this RFP, subject respectively to that chapter or those agreements, but that the rights and obligations of the parties shall be governed by the specific terms of the RFP. In any event of the preceding, all rights under each of those trade agreements, wherever prosecuted, shall be limited to the remedies available in each.

1.8 Competition Act

Under Canadian law, Proposals must be arrived at separately and independently, without conspiracy, collusion or fraud. Please go to website below for further information.
http://www.competitionbureau.gc.ca

2. RFP Scope of Work and the IT Solution

This Section details the goods and services, collectively, forming the IT Solution to be provided under this RFP as well as the requirements of the Partnership for such IT Solution. By submission of a Proposal in response to this RFP, the Proponent is requested to comply with the requirements identified in this Section at the rates identified in the Proponent's Rate Bid Form **(Appendix C)** if selected as the preferred Proponent. Submission requirements are contained within Part 3 of this RFP.

The IT Solution

A high level description of the support services, applications and infrastructure that the contemplated IT Solution will cover are described in the future state section in **Exhibit A**.

The Partnership's requirements with respect to:

(a) Project work requirements and requirements with respect to the IT Solution's design; build; migration; installation; configuration; and implementation are provided in Exhibit "B";

(b) the service desk requirements are provided in Exhibit "C";

(c) the application management requirements including application licenses and monitoring are provided in Exhibit "D";

(d) the managed hosting requirements including uptime, security, privacy; system availability; and disaster recovery are provided in Exhibit "E";

(e) the service level objectives including outage definitions for fee abatements are provided in Exhibit "F"; and

(f) the term sheet compliance are provided in Appendix A.

Out of Scope

The following services can be considered out-of-scope for the purposes of the Agreement.

i. Legal Advisory Services
ii. Privacy Advisory Services
iii. Web Development Services

3. Submission Requirements

3.1 General Overview

i. For the purposes of the requirements stated in this RFP:
"must", and "shall" indicate that the requirement is mandatory, subject to the provisions of this RFP.
"should", "could", and "may" indicate that the requirement is discretionary.

ii. For clarity, the mere use of the term "required" or "requirement" is not, in and of itself, determinative of whether a particular requirement is either a mandatory or discretionary requirement.

iii. In responding to any aspect of this RFP, expressions such as, "have negotiated these concepts in the past with other customers to our mutual satisfaction", "read and understood" or "subject to review/further review by our legal counsel" will not be considered as satisfactory response and will be scored accordingly. Direct answers to questions raised by the RFP are encouraged.

iv. Proposals are expected to address the RFP content requirements as outlined herein, and should be ordered, detailed and comprehensive. Clarity of language, adherence to the suggested structuring and adequate accessible documentation is essential to the Partnership's ability to conduct a thorough evaluation. The Partnership is interested in Proposals that demonstrate efficiency and value for money.

v. General marketing and promotional material will not be reviewed or considered.

vi. The Partnership prefers that the assumptions used by a Proponent in preparing its Proposal are kept at a minimum and that Proponents will ask for clarification prior to the deadline for the Proponent questions rather than make assumptions to the extent possible. Proponents should also review all documents including all Exhibits.

vii. Where a Proponent's assumptions are inconsistent with information provided in the RFP, or so extensive that the total Proposal cost is unqualified, such Proponent risks disqualification by the Partnership in its sole discretion.

3.2 Proposal Content

The following table describes the format and content of each Proponent's Proposal to be submitted in response to this RFP. Where an item is referring to an Appendix, the Proponent should use the referenced Appendix for its response.

Item	Appendix to Complete	Description
Table of Contents	N/A	Include page numbers and identify all included materials in the Proposal.
Covering Letter	N/A	Include a covering letter to your proposal providing an overview of your company, the

		team you are proposing and why you are a good fit for this project. Recommended length 1 page.
Corporate Overview	N/A	Provide a description of your organization including size, organization and structure. An organizational chart should be included. Recommended length 2 pages.
Overview of the IT Solution	N/A	Provide an overview of your proposed IT Solution including the following information: • Proposed approach and plan to successfully complete the transition project work by March 31, 2017 • A description of the Proponent's commitment to the Partnership's IT Solution and successfully maintaining a customer-focused, high quality service over the 5 -7 year contract period. Recommended length 3 pages.
Experience and Qualifications	N/A	Provide a description and demonstrate your experience and qualifications as required for the successful completion of the Services described in this RFP. Recommended length 3 pages.
Overview of Team	N/A	Provide an overview of your proposed team including a high-level summary of the size of your team and their areas of expertise, an overview of your internal reporting structure, and how you plan to meet the requirements as outlined in the RFP. Resumes for all Implementation and Support Service Team Members included in the Proposal should be submitted. Recommended length of 2 pages per individual resume.
Overview of Project Management Methodology and Transition Work Plan	N/A	Provide an overview of your project management methodology including how your team develops the project plan, the project documentation created, how the project is

		tracked, project status reports, and risk/issue tracking processes. A detailed project work plan for the transition work between January 2, 2017 and March 31, 2017 should be provided.
Project Work Requirements	N/A	Provide a written response to each of the requirements listed in Exhibit B.
Service Desk Requirements	N/A	Provide a written response to each of the requirements listed in Exhibit C.
Application Management Requirements	N/A	Provide a written response to each of the requirements listed in Exhibit D.
Managed Hosting Requirements	N/A	Provide a written response to each of the requirements listed in Exhibit E.
Service Level Objective Requirements	N/A	Provide a written response to each of the requirements listed in Exhibit F.
Term Sheet Compliance	Appendix A	Please complete and submit as part of the Proposal.
Form of Offer	Appendix B	**Mandatory Form** to be completed and submitted as part of the Proposal.
Rate Bid Form	Appendix C	Please complete and submit as part of the Proposal. **Note: The Rate Bid Form should be submitted as a separate document.**
Client Reference Form	Appendix D	Please complete and submit as part of the Proposal.

4. Terms and Conditions of the RFP Process

4.1 RFP Timetable and Process

The following is the schedule for this RFP:

RFP ISSUE DATE	**Monday, September 12, 2016**
1 UNIVERSITY AVE. OFFICE SITE VISIT	**Friday, September 30, 2016 from 12:00:00 to 1:00:00 p.m. local Toronto time**
INFORMATION SESSION	**Friday, September 30, 2016, from 1:00:00 to 3:00:00 p.m. local Toronto time**
DEADLINE FOR PROPONENT ENQUIRIES	**Thursday, October 6, 2016 no later than 3:00:00 p.m. local Toronto time**
DEADLINE FOR ISSUING ADDENDA & RESPONSES TO PROPONENT ENQUIRIES	**Tuesday, October 11, 2016 by 4:00:00 p.m. local Toronto time**
PROPOSAL SUBMISSION DEADLINE	**Thursday, October 20, 2016 no later than 3:00:00 p.m. local Toronto time**
PROPONENT INTERVIEWS	**Week of November 7, 2016**

All times specified in this RFP timetable are local times in Toronto, Ontario, Canada.

The Partnership may change the RFP timetable in its sole and absolute discretion at any time prior to the Proposal Submission Deadline. The Partnership may amend any timeline, including the Proposal Submission Deadline, without liability, cost, or penalty, and within its sole discretion.

In the event of any change in the Proposal Submission Deadline, the Proponents may thereafter be subject to the extended timeline.

In the event a change is made to any of the above dates, the Partnership will post notice of any such change on the Partnership website, Biddingo™ and MERX.

4.2 General Information and Instructions

i. This RFP is available only through the Partnership website, Biddingo™ and MERX, the electronic tendering system used in the Province of Ontario. For further information about Biddingo™ or MERX, visit the Biddingo™ website at http://www.biddingo.com/ or the MERX website at http://www.merx.com/

ii. All Proposals are to be in English only. Any Proposals received by the Partnership that are not entirely in the English language may be disqualified.

iii. Proponents should structure their Proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a Proposal should reference the applicable section numbers of this RFP where that request was made.

iv. Proponents should submit their Proposals in two separate parts. The financial part will contain the price portion of the Proposal using the Rate Bid Form, in Appendix C. The technical part will contain the rest of the Proposal. Each part should be submitted in a separate sealed package or electronic file in accordance with the instructions in this Section.

v. Proponents **should** submit **seven** printed hard copies of the Proposal with original signatures. It should be packaged in a sealed envelope and labelled with the Proponent's name and address. A hard copy of the Proposal with an original signature **Must** be delivered to the address below before the Proposal Submission Deadline set out in Section 4.1:

Canadian Partnership Against Cancer Corporation
1 University Ave, Suite 300
Toronto, ON M5J 2P1
Attention: Samoya Lloyd

vi. Proponents should also submit one electronic copy in Microsoft Word format or portable document format (PDF), sent by e-mail to procurement@partnershipagainstcancer.ca before the Proposal Submission Deadline. Proposals submitted in any other manner may not be accepted.

vii. In the event of conflict or inconsistency between the hard copy and the electronic copy of the Proposal, the electronic copy of the Proposal shall prevail, if provided before the Proposal Submission Deadline. **Both the hard copy and electronic copy should be submitted before the Proposal Submission Deadline.** It is the sole responsibility of the Proponent to ensure the hard copy and the electronic copy are received by the Partnership, before the Proposal Submission Deadline.

4.3 Office Site Visit and Information Session

An office site visit will be held at the following location on Friday September 30, 2016 at noon until 1PM:

1 University Avenue
Suite 300
Toronto, ON
M5J 2P1

Proponents are strongly encouraged to attend as the office site visit will likely assist each Proponent in preparing their Proposal.

Immediately following the office site visit, an information session will be held at 1PM at the same location. At this information session, some or all of the Proponents' questions received prior to the session may be responded to. Questions may also be asked at the information session which the Partnership may elect to answer. Any oral responses by the Partnership shall be non-binding. Only a subsequent Addendum including the question and answer, if any, will form part of this RFP.

Proponents are strongly encouraged to attend the information session.

5. Evaluation Process and Criteria

Proposals will be reviewed and evaluated by an evaluation committee which is comprised of representatives of the Partnership and may include external advisors (the **"Evaluation Committee"**). The Partnership will conduct the evaluation of proposals as detailed in the table below (the **"Evaluation Process and Criteria Table"**).

Stage		Evaluation	Weight
1	**Mandatory Criteria** **Proponents must meet all Mandatory Criteria to proceed to Stage 2.**	**Pass/Fail**	**Pass**
2	**Rated Evaluation** **(a) The three (3) highest scoring Proponents who achieve a minimum required score of 70% under Stage 2 will proceed to Stage 3.** **(b) If there are less than 3 Proponents who achieve a minimum required score of 70% then, subject to the 3 Proponent maximum, each Proponent within 5 points of the highest and/or second highest scoring Proponent will proceed to Stage 3 even if they score below 70%.** **(c) Subject to (a) and (b), if there is a tie between the third and fourth highest scoring Proponents, the Proponent with the highest score in Stage 2A will proceed to Stage 3.**	**Rated**	**110 points**
2A	Proponent Commitment to IT Solution, including strategic ability to fit to a successful implementation and sustainment of a high quality, continuously improving IT Solution over the 5-7 year contract period.	Rated	10 points
2B	Qualifications and experience of the Proponent organization • Depth of resourcing and maturity of Service Desk processes • Compatibility with the Partnership's culture • Commitment to continuous improvement	Rated	10 points

	• Commitment to Customer-focused Service • Quality and Relevancy of Client References		
2C	Qualifications and experience of key members of the proposed implementation and support service team The Proponent **should** provide a resume for each team member that will fulfil an implementation or support service role as part of their Proposal. Where a single resource is fulfilling multiple roles, the resume should only be submitted once.	Rated	20 points
2D	Quality of the proposed approach and work plan (adequacy of project team structure, work plan, client engagement, reporting and controls, likelihood of timely delivery) for transition period (January 2017-March 31, 2017) The Proponent **should** provide a detailed Work Plan as part of their Proposal.	Rated	20 points
2E	Compliance with Service Desk, Application Management, Managed Hosting and Service Level Objective Requirements	Rated	40 points
2F	Compliance with Term Sheet	Rated	**10 points**
3	**Interviews**	**Rated**	**40 points**
4	**Pricing Evaluation** **Net present value calculation – 40 points** **Rate Card - 10 points**		**50 points**
Total Score (cumulative)			**200 points**

5.1 Stage 1 - Mandatory Criteria

First, the Partnership will evaluate Proposals for compliance with the following mandatory criteria (the "**Mandatory Criteria**"):

Requirement Title	Submission Details
Delivery Location for RFP	All Proposals **Must** be submitted as stated in Section 4.2.
Proposal Submission Deadline	RFPs **Must** be submitted prior to the Proposal Submission Deadline as stated in Section 4.1.
Form of Offer (Appendix B)	Each Proposal **Must** include a Form of Offer (Appendix B) completed and signed by an authorized representative of the Proponent.

Any Proposal that does not meet the Mandatory Criteria will be disqualified. If a Proposal is disqualified, it will not be further evaluated.

(a) Form of Offer (Appendix B)

Each Proposal **Must** include a Form of Offer (Appendix B) completed and signed by the Proponent.

In addition to the other information and representations made by each Proponent in the Form of Offer, each Proponent must declare whether it has an actual or potential unfair advantage in relation to the submission of its Proposal or a Conflict of Interest in relation to the performance of its contractual obligations contemplated in the RFP.

If, at the sole and absolute discretion of the Partnership, the Proponent is found to have an actual or potential unfair advantage or Conflict of Interest, the Partnership may, in addition to any other remedies available at law or in equity, disqualify the Proposal submitted by the Proponent.

The Proponent, by submitting the Proposal, warrants that to its best knowledge and belief that it has no (i) actual or potential unfair advantage with respect to the submission of its Proposal; or, (ii) actual or potential Conflict of Interest in the performance of its contractual obligations contemplated in the RFP other than those disclosed in the Form of Offer.

Where the Partnership discovers a Proponent's failure to disclose actual or potential unfair advantage or Conflict of Interest, the Partnership may disqualify the Proposal or terminate any Agreement awarded to that Proponent pursuant to this procurement process. The Partnership shall determine, on a case by case basis, whether the actual unfair advantage/Conflict of Interest or potential unfair advantage/Conflict of Interest, disclosed pursuant to this RFP is material and whether it shall result in disqualification of the Proposal.

The Partnership, in addition to any other remedies it may have in law or in equity, shall have the right to rescind any contract awarded to a Proponent in the event that the Partnership

determines that the Proponent made a misrepresentation or submitted any inaccurate or incomplete information in the Form of Offer.

Other than inserting the information requested and signing the Form of Offer, a Proponent may not make any changes to or qualify the Form of Offer in its Proposal. A Proposal that includes conditions, options, variations or contingent statements that are contrary to or inconsistent with the terms set out in the RFP may be disqualified. If a Proposal is not disqualified despite such changes or qualifications, the provisions of the Form of Offer as set out in this RFP will prevail over any such changes or qualifications in or to the Form of Offer provided in the Proposal.

5.2 Stage 2 - Rated Criteria

Next, the Partnership will evaluate and score Proposals based on the Evaluation Process and Criteria Table (the "**Rated Criteria**"):

NOTE: The Partnership reserves the right to revise the minimum required score threshold, if not enough Proposals have met the threshold.

(a) Compliance with Term Sheet (Appendix A)

The Proponent should review and provide a response to each of the items included in the Term Sheet provided in Appendix A in the format provided. For review purposes, a full copy of the Term Sheet is set out in **Exhibit "G".**

The Proposal should include the information requested in the format provided including (i) whether or not the Proponent accepts the Term as stated in the Term Sheet Compliance (Appendix A) in whole or in part and (ii) where a Proponent either accepts in part or where they do not accept the Term, they should provide suggestions for specific changes that would make the Term acceptable.

Expressions such as but not limited to "have negotiated these concepts in the past with other customers to our mutual satisfaction", "read and understood" or "subject to review/further review by our legal counsel" will not be considered as being clear and specific alternatives.

(b) Rate Bid Form (Appendix C)

Each Proponent should include the completed forms according to the instructions contained in the forms as well as those instructions set out below:

i. A separate file should be submitted containing the financial proposal.

ii. Prices should be provided in Canadian Funds;

iii. Except for Harmonized Sales Tax (HST) as specified in the Rate Bid Form (Appendix C), prices quoted by the Proponent should be all inclusive.

iv. The Rate Bid Form (Appendix C) included in the RFP should not be altered in any way other than by insertion of the required information in the fields provided.

v. Proponents should provide pricing in Appendix C by completing the required tables.

The pricing evaluation separates pricing elements according to the project's implementation and ongoing cost of support services. For scoring purposes, two primary valuations will be made

- Net present value calculation and
- Rate Card.

A failure to use the Rate Bid Form in whole or in part, or to follow the instructions associated with the Rate Bid Form, or the making of assumptions in the Rate Bid Form, that are inconsistent with the terms of this RFP, will likely prejudice the Proponent's Proposal and Proponents are advised to take appropriate care. The Partnership has no obligation to look beyond the Rate Bid Form in scoring pricing and can take such steps to normalize pricing based on Proponent's assumptions as it may determine is appropriate in the circumstances. A failure to provide all information required by the Rate Bid Form will likely result in the Partnership making pricing assumptions and normalizations that will negatively impact the scoring of Proponent's Proposal, and perhaps in a material way.

Proponents should include a listing of the assumptions upon which the pricing in its Proposal is based, and such assumptions should be consistent with the information provided in this RFP and should be entered only in the space provided in Rate Bid Form. In addition to scoring specific cost values provided by the Proponent, the Partnership will also be objectively evaluating the pricing methodology and appropriateness of pricing assumptions.

(c) Client Reference Form (Appendix E)

The Proponent **should** provide a completed Client Reference Form (Appendix E) as follows:

- One (1) reference where the Proponent has had a long-term (> 5 years) relationship for IT Support Services.
- Two (2) references for Microsoft Azure Cloud Managed Services
- Two (2) references for IT Service Desk Services

5.3 Stages of the Proposal Evaluation

The Partnership may conduct the evaluation of Proposals in the following four (4) stages:

Stage 1

Stage 1 will consist of a review to determine which Proposals comply with all of the Mandatory Criteria. Proposals which do not comply with all of the Mandatory Criteria, will, subject to the express and implied rights of the Partnership, be disqualified and not be evaluated further. Proponents must meet all Mandatory Criteria to proceed to Stage 2.

Stage 2

Stage 2 may consist of a scoring by the Partnership of each qualified Proposal on the basis of the Rated Criteria as outlined in Section 5.2.

Stage 3

(a) The three (3) highest scoring Proponents who achieve a minimum required score of 70% under Stage 2 will proceed to Stage 3.

(b) If there are less than 3 Proponents who achieve a minimum required score of 70% then, subject to the 3 Proponent maximum, each Proponent within 5 points of the highest and/or second highest scoring Proponent will proceed to Stage 3 even if they score below 70%.

(c) Subject to (a) and (b), if there is a tie between the third and fourth highest scoring Proponents, the Proponent with the highest score in Stage 2A will proceed to Stage 3.

The Partnership will shortlist the top 3 scoring Proposals and their respective Proponent organizations may be invited to an interview at the Partnership offices. Interviews to be scheduled, at a time that is convenient for the Partnership.

Stage 4

Upon completion of Stage 3 for all Proposals, the sealed pricing envelope provided by the Proponent(s) that meet the minimum required score will then be opened and Stage 4 may consist of a scoring of the pricing submitted. The evaluation of price may be undertaken after the evaluation of Mandatory Criteria (Stage 1), any Rated Criteria (Stage 2) and the Interviews (Stage 3) has been completed. The formula to be used for scoring price is as follows for each of the net present value calculation and the Rate Card:

S = MP x L / P, where:

S = the price score for the Proposal being evaluated;
MP = the maximum points awarded for price;
L = the price of the lowest price remaining Proposal; and
P = the price of the Proposal being scored.

5.4 Cumulative Score

At the conclusion of Stage 4, the scores from Stage 2, Stage 3 and Stage 4 will be added and, subject to satisfactory reference checks and the express and implied rights of the Partnership, the highest scoring Proposal will be selected and the Proponent of that Proposal will be invited to enter into the Agreement in accordance with Section 1.5.

The Partnership intends to award an Agreement to the Proponent who submits the most advantageous Proposal to the Partnership as determined by the Partnership through the evaluation process.

The Proposal with the lowest price will not necessarily be selected. While price is a determinant in the selection process, it is to be clearly understood that there should be a full and complete understanding of the IT Solution to be provided, demonstrated through the Proposal as presented, as well as a commitment to the Agreement terms and conditions set out in **Appendix "A"**. It is the intention of the Partnership to enter into an Agreement with the Proponent providing the best value to the Partnership as identified through the evaluation process.

If no Proponents demonstrate appropriate qualifications or experience, the Partnership may, without liability cost or penalty, cancel this RFP or choose not to award an Agreement to any of the Proponents.

5.5 Tie Breaker

The Proposal that achieves the highest Total Score will be ranked first. In the event of a tie of Total Score, the Proponent achieving the highest score in Stage 2 – Rated Criteria will be ranked first overall. In the event that a tie still remains, the Proponent achieving the highest score in the Interview Stage 3 will be ranked first overall.

5.6 Pricing

Using the Rate Bid Form, please submit the price for completion of this project (both fees and expenses). The Proponent should assume that it is required to supply all necessary professional staff to undertake the project. The Proponent should submit pricing (Appendix C) in a separate sealed package or separate electronic file from the rest of the Proposal (see Section 3.2).

5.7 AODA Compliance Legislation

As part of its response to this RFP, a Proponent may describe all measures that the Proponent intends to implement or make available in order that the IT Solution provided in response to this RFP be in compliance with applicable standards under the Accessibility for Ontarians with Disabilities Act, 2005 ("**AODA**") and its regulations, including but not limited to (i) any training that has been, or will be, provided to Proponent's staff; and (ii) all policies implemented by the Proponent in respect of the AODA and its regulations. The Agreement shall require that the successful Proponent provide the IT Solution in accordance with AODA and its regulations.

6. SUPPLEMENTARY TERMS AND CONDITIONS

The Partnership may amend the schedule for this RFP in its sole discretion at any time prior to the Proposal Submission Deadline.

6.1 All New Information to Proponents by way of Addenda

This RFP may be amended only by a written addendum (an "**Addendum**") in accordance with this Section. If the Partnership, for any reason, determines that it is necessary to provide additional information relating to this RFP, such information will be communicated to all Proponents by Addenda made available to all Proponents in the same way as the original RFP. Each Addendum shall form an integral part of this RFP.

Such Addenda may contain important information including significant changes to this RFP. Proponents are responsible for obtaining all Addenda issued by the Partnership.

Any amendments or supplements to this RFP made in any other manner shall not be binding. **It is the sole responsibility of the Proponent to ensure that it has received all Addenda pertaining to this RFP.** The Partnership will not take any responsibility for losses, misunderstandings, errors or omissions from the Proponent not having received or reviewed any and all Addenda.

Proponents who intend to respond to this RFP are requested not to cancel the receipt of Addenda or Amendments option provided by Biddingo™ or MERX, since they should obtain all of the information documents that are issued through Biddingo™, MERX or the Partnership website.

In the event that a Proponent chooses to cancel the receipt of Addenda or Amendments option, its Proposal may be rejected.

6.2 Ownership of Proposals

Unless received after the RFP Submission Deadline, all information obtained by the Partnership from Proponents in connection with this RFP will remain with the Partnership and be retained for internal purposes and the Partnership will not return the Proposal or any accompanying documentation submitted by a Proponent. Information provided by Proponents in response to this RFP may be disclosed by the Partnership if permitted or required by law.

6.3 Governing Law of RFP Process

The RFP process shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein.

6.4 Proponents to Follow Instructions

Proponents should structure their Proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a Proposal should reference the applicable section numbers of this RFP where that request was made. Proponents responding to the RFP should provide additional information related to contacts and their corporate identity and status.

- The Proponents ***must*** submit a signed Form of Offer in the form of Appendix B with its Proposal.

- The Proponent should identify a single point of contact through which all communications from the Partnership will be channeled.

- The legal status (incorporation, partnership, etc.) and registered legal name of the Proponent be clearly identified in the Proposal, along with the name, title and telephone number of the individual who will be the Proponent's signing authority for the Agreement. Proponents should also include their HST number or the relevant information required for taxation purposes.

6.5 Partnership's Information in RFP only an Estimate

The Partnership and its advisors make no representation, warranty or guarantee as to the accuracy of the information contained in this RFP or issued by way of Addenda. Any quantities shown or data contained in this RFP or provided by way of Addenda are estimates only and are for the sole purpose of indicating to Proponents the general size of the work.

It is the Proponent's responsibility to avail itself of all the necessary information to prepare a Proposal in response to this RFP.

6.6 Proponents Shall Bear Their Own Costs

The Proponent shall bear all of its own costs associated with or incurred in the preparation, presentation and submission of its Proposal including, if applicable, costs incurred for interviews, site visits or demonstrations.

6.7 Communication after Issuance of RFP

Proponents shall promptly examine all of the documents comprising this RFP and shall report any errors, omissions or ambiguities, and may direct questions or seek additional information by e-mail to the e-mail address set out in Section 6.8, before the Deadline for Proponent Enquiries set out in Section 4.1. Proponents should submit all questions via e-mail. No such communications are to be directed to the Partnership in any other manner. It is the responsibility of the Proponent to seek clarification from the Partnership on any matter it considers to be unclear. The Partnership is under no obligation to provide additional information; but, may do so at its sole discretion.

6.8 RFP Contact Information

All communications regarding any aspect of this RFP should be directed to the following RFP Contact:

Name: **Samoya Lloyd**

Title: **Manager, Procurement**

Email: Procurement@partnershipagainstcancer.ca

Proponents that fail to comply with the requirement to direct all communications to the RFP Contact may be disqualified from RFP process. Without limiting the generality of this provision, Proponents shall not communicate with or attempt to communicate with the following:

- any member of the Partnership evaluation team for the RFP;
- any expert or advisor assisting the Partnership evaluation team;
- any employee or agent of the Partnership (other than the RFP Contact)
- any member of the Partnership's governing body (such as Board of Governors, Board of Directors, Board of Advisors or Trustees)
- any elected official of any level of government, including any advisor to any elected official

6.9 Partnership May Seek Clarification and Incorporate Response into Proposal

The Partnership reserves the right, but is not obliged, to verify or seek clarification and supplementary information relating to the verification or clarification from Proponents after the Proposal Submission Deadline including those related to an ambiguity in a Proposal or in any statement made subsequently during the evaluation process. The response received by the Partnership from a Proponent shall, if accepted by the Partnership, form an integral part of that Proponent's Proposal. However, Proponents are cautioned that any verifications or clarifications sought will not be an opportunity either to correct errors or change their Proposals in any substantive manner.

Verifications or clarifications under this subsection may be made by whatever means the Partnership deems appropriate and may include contacting, any person identified in the Proposal and persons or entities other than those identified by any Proponent. In submitting a Proposal, a Proponent is deemed to consent to the Partnership's verification or clarification rights.

In the event that the Partnership receives information at any stage of the evaluation process which results in earlier information provided by the Proponent being deemed by the Partnership to be inaccurate, incomplete or misleading, the Partnership reserves the right to revisit the Proponent's compliance with the Mandatory Criteria and/or adjust the scoring of Rated Criteria.

6.10 RFP Incorporated into Proposal

All of the provisions of this RFP and its appendices are deemed to be accepted by each Proponent and incorporated into each Proponent's Proposal.

6.11 No Incorporation by Reference by Proponent

The entire content of the Proponent's Proposal should be submitted in a fixed form. The content of websites or other external documents referred to in the Proponent's Proposal will not be considered to form part of its Proposal.

6.12 Confidentiality

All information received by the Proponent provided by or obtained from the Partnership in any form in connection with this RFP either before or after the issuance of this RFP:

- is the sole property of the Partnership and must be treated as confidential;
- is not to be used for any purpose other than replying to this RFP and the performance of any subsequent Agreement;
- must not be disclosed without prior written authorization from the Partnership; and
- shall be returned by the Proponent to the Partnership immediately upon the request of the Partnership.

6.13 Disqualification

The Partnership may disqualify a Proposal on grounds of faulty submission, improper conduct or provision of inaccurate or misleading information by the Proponent.

6.14 Reserved Rights

The Partnership, without liability, cost or penalty reserves the right to:

i. make public the names of any or all Proponents;
ii. request written clarification or the submission of supplementary written information in relation to the clarification request from any Proponent and incorporate a Proponent's response to that request for clarification into the Proponent's Proposal.
iii. amend or supplement this RFP at any time prior to seven (7) calendar days before the Proposal Submission Deadline;
iv. reject any or all Proposals in its absolute discretion;
v. if a single Proposal is received, reject the Proposal of the sole Proponent and cancel this RFP process or enter into direct negotiations with the sole Proponent;
vi. discuss with any Proponent different or additional terms to those contemplated in this RFP or in any Proponent's Proposal;
vii. verify with any Proponent or third party any information set out in a Proposal;
viii. check references other than those provided by any Proponent;

ix. disqualify any Proposal that contains misrepresentations or any other inaccurate or misleading information;
x. select any Proponent other than the Proponent whose Proposal reflects the lowest cost to the Partnership or the highest overall score;
xi. make changes, including substantial changes, to this RFP provided that those changes are issued by way of Addenda in the manner set out in this RFP;
xii. accept any Proposal in whole or in part;
xiii. accept Proposals from more than one Proponent;
xiv. negotiate in respect of any term or condition proposed by the Proponent in its Proposal, whether a business or legal term or condition or otherwise;
xv. cancel this RFP process at any stage;
xvi. cancel this RFP process at any stage and/or issue a new RFP for the same or similar services or deliverables or IT Solution;
xvii. disqualify any Proponent or the Proposal of any Proponent who has engaged in conduct prohibited by this RFP;
xviii. adjust the scoring of or reject a Proponent's Proposal on the basis of:
    1) a financial analysis determining the actual cost of the Proposal when considering factors including quality, service, price and transition costs arising from the replacement of existing goods, services, practices, methodologies and infrastructure (howsoever originally established);
    2) information provided by references;
    3) the Proponent's past performance on previous contracts awarded by the Partnership;
    4) the information provided by a Proponent pursuant to the Partnership exercising its clarification rights under this RFP process; or
    5) other relevant information that arises during this RFP process; or
xix. Waive non-compliance where, in the Partnership's sole and absolute discretion, such non-compliance is minor and not of a material nature, or to accept or reject in whole or in part any or all Proposal, with or without giving notice. Such minor non-compliance will be deemed substantial compliance and capable of acceptance. The Partnership will be the sole judge of whether a Proposal is accepted or rejected.

This RFP is not an offer to enter into a bidding contract (often referred to as "Contract A") or a contract to carry out the services contemplated in this RFP (often referred to as "Contract B"). Neither this RFP nor the submission of a response nor its receipt by the Partnership shall create any contractual rights or obligations whatsoever on either the Partnership or any Proponent, nor oblige the Partnership in any manner whatsoever.

6.15 Bait and Switch

By submitting a Proposal the Proponent agrees and acknowledges that it will provide for the duration of the project, the full complement of staff required to perform the work of the project, including the specific individuals identified in its Proposal. The Proponent agrees to provide all professional personnel necessary to perform the scope of work, including those who are named in the Proposal submitted in response to the Partnership's RFP. These key

personnel shall remain assigned for the duration of the project, unless otherwise agreed to in writing by the Partnership. In the event the Proponent wishes to substitute any of the key personnel, the individual(s) proposed should demonstrate similar qualifications and experience as required to successfully perform such duties. The Partnership shall have the sole right to determine whether key personnel proposed as substitutes are qualified to work on the project. The Partnership shall not unreasonably withhold approval of staff changes.

7. Execution of Agreement, Notification and Debriefing

7.1 Selection of Proponent

The Partnership has the discretion to conduct contract negotiations in such manner as it will determine. That said, it is anticipated that the Partnership will select one (1) Proponent, the highest ranked Proponent, with whom the Partnership will commence contract negotiations.

It is anticipated that a second Proponent, the second highest ranked Proponent, will be held in abeyance pending the result of the negotiations with the first Proponent. Following the approval of the negotiated contract by the Partnership, the name of the selected Proponent, duration of awarded contract, and options for contract extension will be posted to the Partnership's Website, Biddingo™ and MERX™.

7.2 Notification to Other Proponents

Once the preferred Proponent and the Partnership execute the Agreement, the other Proponents will be notified by the Partnership in writing (and in some procurements on the Biddingo™ and/or Merx™ system) of the outcome of the procurement process, including the name of the preferred Proponent, and the award of the Agreement to the preferred Proponent.

7.3 Debriefing

Proponents may request a debriefing after receipt of a notification of award. All requests must be in writing to the RFP Contact set out at Section 6.8 of this RFP and must be made within sixty (60) days of notification of award. The intent of the debriefing information session is to aid the Proponent in presenting a better Proposal in subsequent procurement opportunities. Any debriefing provided is not for the purpose of providing an opportunity to challenge the procurement process.

7.4 Bid Dispute

Any dispute, complaint, or protest (a **"Bid Protest"**) in respect of this RFP by a Proponent, including, without limitation, the awarding of any Agreement to another Proponent or otherwise, shall be addressed by the Proponent solely through a notice to the RFP Contact, in writing, referring to this Section of the RFP and setting out the particulars of the Bid Protest.

The Bid Protest shall be recorded and acknowledged by the RFP Contact on behalf of the Partnership in a prompt manner.

A response to the Bid Protest will be developed by the Partnership and may involve such personnel from the Partnership at an appropriate level as are reasonably required to provide a response to the Bid Protest.

The Partnership may wish to seek clarifications before providing a response, and reserves the right to delay providing a response until the Agreement has been entered into by the Partnership and the contracted Proponent.

7.5 Prohibited Proponent Communications

Proponents **shall** address all questions and requests for clarification with respect to their Proposals, or the RFP documents or the RFP process only to the RFP Contact set out in Section 6.8.

Proponents **shall**, in accordance with Section 6.8 of this RFP**,** not contact or make any attempt to contact, (a) any Partnership employee or representative, other than the RFP Contact; or (b) any other Proponent with respect to a Proposal, the RFP documents, or the RFP process, at any time during the RFP process.

(a)

on matters related to their Proposals, the RFP documents, or the RFP process at any time during the RFP process.

7.6 Proponent Not to Communicate With Media

A Proponent may not at any time directly or indirectly communicate with the media in relation to this RFP or any Agreement awarded pursuant to this RFP without first obtaining the written permission of the RFP Contact set out at Section 6.8 of this RFP.

(a)

7.7 Personal Health Information and Protection of Privacy Act (PHIPA)

The Partnership is committed to protecting the privacy of Personal Health Information (PHI) in accordance with PHIPA, other applicable legislation and standards, and the expectations of applicable regulatory authorities for privacy such as the Privacy by Design principles of the Information and Privacy Commissioner of Ontario.

The successful Proponent will be subject to the requirements imposed on providers of information technology and information management services to health information custodians, in the regulations under PHIPA (and any other applicable legislation) and under the Agreement.

For more information on privacy provisions with which the successful Proponent will be requested to comply, see Appendix A – Term Sheet Compliance.

APPENDIX A – TERM SHEET COMPLIANCE

APPENDIX A – TERM SHEET COMPLIANCE

Item No.		Letter Agreement with Attached Term Sheet for IT Solution	Response	Exceptions
1.	A. Confirm that Proponent agrees to the concept of a LOA-TS. If the answer is not an unqualified yes, then a clear and specific alternative should be provided. Expressions such as but not limited to "have negotiated these concepts in the past with other customers to our mutual satisfaction", "read and understood" or "subject to review/further review by our legal counsel" will not be considered as being clear and specific alternatives.			
2.	B. Confirm that Proponent agrees to each of the following terms of the LOA-TS being incorporated into the TS-LOA. If the answer is not an unqualified yes, then a clear and specific alternative should be provided. Expressions such as but not limited to "have negotiated these concepts in the past with other customers to our mutual satisfaction", "read and understood" or "subject to review/further review by our legal counsel" will not be considered as being clear and specific alternatives. Please use Appendix A (Term Sheet Compliance) as a tool to provide context to the following provisions as against the TS-LOA as a whole.			
3.	To facilitate the preparation and negotiation of Definitive Agreements (as defined below in section 1), this Letter of Agreement - Term Sheet (LOA-TS) (the "Letter of Agreement - Term Sheet (LOA-TS)") dated [DATE] (the "Effective Date") is intended to generally describe the fundamental business terms for the proposed [hosting], licensing, implementation (including configuration and training),			

Item No.		Letter Agreement with Attached Term Sheet for IT Solution	Response	Exceptions
	and ongoing maintenance and support of an information technology system ("IT Solution") by ["x"] ("Supplier") to Canadian Partnership Against Cancer Corporation ("Partnership"). On the basis of this LOA-TS, a definitive agreement between the parties can be prepared and negotiated. No party shall have any legal obligation or liability in respect of Section 1 below to the other unless and until the applicable definitive agreements (the "Definitive Agreement(s)", as further defined in Section 1 below) are executed by duly authorized representatives of each party. To the extent that a party incurs expenses or liabilities in reliance on negotiating the Definitive Agreement, it does so at its own risk in the event the Definitive Agreement is not executed.			
4.	No party shall have any legal obligation or liability in respect of Section 1 below to the other unless and until the applicable Definitive Agreements are executed by duly authorized representatives of each party. To the extent that a party changes its position in reliance on negotiating the Definitive Agreements, it does so at its own risk in the event the Definitive Agreements are not executed.			
5.	The parties agree as follows:			
6.	1. Form and Timing of Definitive Agreement.	The parties shall endeavour to negotiate the Definitive Agreement that shall include, in substantial form, those terms and conditions set out in Schedule "A" (the "Letter of Agreement - Term Sheet (LOA-TS)") to this Letter of Agreement - Term Sheet (LOA-TS). The Partnership shall prepare the first draft of the Definitive Agreement within ["x"] days of the Effective Date. The parties agree to negotiate in good faith to finalize the Definitive Agreement within ["x"] days from the date the Partnership provides Supplier with the first draft.		

Item No.		Letter Agreement with Attached Term Sheet for IT Solution	Response	Exceptions
7.		Upon mutual agreement, Supplier shall bring to the Partnership's location (as reasonably required), its personnel with the authority to finalize the negotiation of all material terms to the Definitive Agreement. Either party may terminate negotiations at any time prior to the execution of the Definitive Agreement on notice to the other party.		
8.	2. Publicity.	No party shall make any public statement or issue any press release concerning the Letter of Agreement - Term Sheet (LOA-TS), the Definitive Agreement or the fact that negotiations are taking place without the consent of the other party, except as may be necessary, in the opinion of counsel, to comply with the requirements of applicable law. If any such public statement or release is so required, the party making such disclosure shall, to the extent practicable, consult with the other party prior to making such statement or release and each party shall use all reasonable efforts, acting in good faith, to agree upon the text of such statement or release. If a party is subject to a legal requirement to make disclosure, that party shall have the final determination as to the timing and content of such disclosure.		
9.	3. Confidentiality.	Each party agrees to use the same degree of care to protect the confidentiality and security of any documents, materials and information which by their nature ought to be treated as confidential and which belong the other parties ("Confidential Information") from disclosure to third parties as it uses to protect its own Confidential Information of similar importance (but in no event less than reasonable care). Disclosure of this Letter of Agreement - Term Sheet (LOA-TS) shall be restricted, in respect of The Partnership and the Supplier, to their: (i) professional advisors and (ii) employees, each of whom to have a need to know. No		

Item No.		Letter Agreement with Attached Term Sheet for IT Solution	Response	Exceptions
		party will be required to keep confidential any Confidential Information that is publicly available without a breach of this Letter of Agreement - Term Sheet (LOA-TS); is lawfully obtained by one of the parties from any third party having legitimate possession of the information disclosed and the right to make such disclosure; or is disclosed by legal requirement, provided that the receiving party provides the disclosing party with reasonable notice of such requirement in order to permit the disclosing party to object to or seek an appropriate order to prevent or limit such disclosure. In the event of the termination of this Letter of Agreement - Term Sheet (LOA-TS), the Confidential Information shared under this Letter of Agreement - Term Sheet (LOA-TS) shall be returned to the disclosing party, or disposed of by a method acceptable to the disclosing party. Each party shall send a letter to the other confirming that the disposal has been done in the agreed manner.		
10.	4. Own Expenses.	The parties shall each be responsible for their own respective costs incurred in connection with the negotiation and entry into of this Letter of Agreement - Term Sheet (LOA-TS) and the Definitive Agreement, including any obligations that such parties may have incurred or otherwise agreed to assume for any finder, consultant, broker or agent in respect of this Letter of Agreement - Term Sheet (LOA-TS) or the Definitive Agreement.		
11.	5. Applicable Law.	This Letter of Agreement - Term Sheet (LOA-TS) shall be interpreted, construed, and governed by and in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein (other than any conflict of law rules that would result in the choice of laws of another jurisdiction) and shall be treated, in all respects, as an Ontario		

Item No.		Letter Agreement with Attached Term Sheet for IT Solution	Response	Exceptions
		contract. The parties agree to submit to the non-exclusive jurisdiction of the courts of Ontario. The parties expressly exclude the application of the United Nations Convention on Contracts for the International Sale of Goods.		
12.	6. Survival.	Sections 2 through 6 shall survive the termination of this Letter of Agreement - Term Sheet (LOA-TS) and the failure or success of the parties to negotiate the Definitive Agreements, unless specifically amended in the Definitive Agreement.		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
13.	A. General Terms of the Definitive Agreements			
14.	1. Orderly and Timely Implementation.	The orderly and timely implementation of the IT Solution is of necessary to the Partnership and shall form a fundamental term of the Definitive Agreement. Orderly and timely implementation is a joint effort that requires the focus and cooperation of all parties and their respective suppliers and agents. Supplier acknowledges the requirement to apply appropriate resources in a timely manner that is consistent with the implementation schedule mutually agreed to by the parties, and also considering that the Partnership may implement the overall IT Solution in multiple phases over time. The Partnership may elect to have specific Supplier personnel involved in the implementation replaced at Partnership's discretion, acting reasonably, and Supplier shall apply		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		appropriate resources to ensure a timely seamless transition in such circumstances.		
15.	2. Ownership and License of Products	In respect of the IT Solution, Supplier grants to the Partnership a perpetual, fully-paid up license that shall permit the use of such IT Solution for the purposes reasonably contemplated by this Agreement. The Partnership may have the IT Solution hosted on its behalf by a third party that agrees to abide by the confidentiality provisions agreed to by the Partnership.		
16.	3. Approval Testing	At the Partnership's request, a specific acceptance testing procedure acceptable to the Partnership and the Supplier will apply that will provide the Partnership with a reasonable period of time to confirm material conformance of the IT Solution with the specifications (including functionality, speed, uptime, interoperability and scalability) provided for in the Supplier's Proposal, in all material respects in a production environment. Such testing may occur in phases to reflect the implementation of the applicable deliverables as part of a system. In respect of acceptance testing, a failure of the IT Solution to successfully pass acceptance testing, within ninety (90) days from the initial start of acceptance testing, will allow the Partnership to terminate the Definitive Agreement for cause and to receive a refund of all amounts paid under the Definitive Agreement.		
17.	4. Maintenance Term.	Subject to early termination for cause and the right of extension by the Partnership for transition, the maintenance and support services for the IT Solution will be available at the Partnership's request, on a year by year basis, for the term of the Definitive Agreement, and including any Transition on Termination provision.		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
18.	5. Transition on Termination.	Following termination, the Partnership may extend the Agreement by up to two (2) years immediately following termination (for cause by either party) to assist in transitioning to a new supplier and the Partnership will pay the Supplier reasonable fees (being the fees in the Agreement, or in the absence of the applicable fee, at the Supplier's then standard published rates) for its services performed during any such transition period. The Partnership will have a perpetual right to use the pre-existing deliverables on termination provided that the license to use the preexisting deliverables has been paid for and termination is unrelated to a continuing and intentional action by the Partnership to violate the intellectual property rights of the Supplier in the IT Solution.		
19.	6. Warranties	Warranties will be provided by Supplier as to skill of staff and standard to which deliverables will perform as part of the overall IT Solution. A warranty will be provided by Supplier as to the sufficiency of any applicable third party components to be compatible and sufficient to meet the specifications set out in the Proposal or such other standard negotiated by the parties. Deliverables to be provided without encumbrances and otherwise to be appropriate to perform to the applicable standard provided for in the Definitive Agreement, including applicable regulatory standards consistent with their reasonably contemplated use under the Definitive Agreement. The warranties and remedies provided shall apply equally to the entire IT Solution, including third party components, and shall continue to apply for so long as the Partnership subscribes for ongoing maintenance and support services. Also warranties as to the provision of virus-free software, the adequacy of applicable source code materials for their contemplated use by the Partnership, and the conformance of all services and other deliverables with applicable law, will be provided by the Supplier. Subject to the		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		Partnership conforming to applicable hardware requirements, there will be a warranty as to the limit of scalability of the IT Solution that is consistent with the other performance and functional specifications of the IT Solution.		
20.	7. Limitation of Liability.	The parties agree to a limitation of liability provision that will only exclude, as to types of damages, a party's right to consequential damages in the nature of loss of profits or loss of revenue and will limit the quantum of damages that are cumulatively available from the other party to the greater of: (i) the amount paid under the Definitive Agreement; and (ii) ten (10) million dollars. Exceptions to any limit on any type or quantum of liability will be provided for (i) breach of confidentiality obligations; (ii) breach of privacy provisions; (iii) damage to tangible or real property or injury or death to persons due to negligence; (iv) intentional misconduct; (v) breach of applicable law; and (vi) the intellectual property indemnity.		
21.	8. Intellectual Property Indemnity.	The Partnership will be held harmless from damages suffered from, and defended by the Supplier, in respect of, any third party intellectual property claim respecting the use of the deliverables provided by Supplier and in the manner contemplated by the Definitive Agreement. Subject to a court injunction binding upon the parties in Ontario that cannot be removed through the best efforts of the Supplier, in all events of intellectual property infringement asserted in respect of the IT Solution, Supplier shall allow the Partnership an additional minimum two year period to continue to use and to migrate to an alternative solution while maintaining the foregoing intellectual property indemnity in respect of such continued use.		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
22.	9. Termination for Cause.	In respect of material breaches, the breaching party will have a sixty (60) day period to correct the breach after notice thereof after which the non-breaching party can terminate immediately on notice. Material breaches can include a series of otherwise non-material breaches of key service level agreements that, over a period of time, culminate into a material breach for which notice can be provided.		
23.	10. SLAs.	Mutually agreed SLAs will be attached to the Definitive Agreement to measure all material forms of performance against specific standards. There will be set-offs against the fees on a prospective basis for a failure to meet the SLAs of a range of 5% (going to 10% for a quarter to quarter failure to meet the 5% SLA) to 25% of the applicable maintenance fees as well as a right to terminate if a recurring failure is a material breach of the Definitive Agreement and it is not corrected within the applicable period of time. Both uptime and response times are of fundamental importance. The hardware and associated components that will provide the required sub-second response time to ensure optimal performance and reliability will be mutually agreed upon by Supplier and hardware/network provider and described in this TS-LOA and thereafter in the Definitive Agreement. Supplier's SLA in this respect is limited only to performance "within the box", ie application and database configuration, unless hosting services are provided by Supplier, in which event such elements shall also be incorporated into the SLAs. Schedule "B" includes details on uptime and response time requirements.		
24.	11. Security and Confidentiality.	The Partnership is subject to privacy requirements, and the Supplier shall at all times comply strictly with the Definitive Agreement in such manner as to ensure that its acts or omissions do not result in the Partnership being in violation of any applicable privacy requirements. No ownership rights in any information or data that the Supplier may have		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		access to by virtue of the Definitive Agreement shall accrue to the Supplier. Schedule "C" shall be used in respect of the privacy provisions. Supplier will provide reasonable co-operation and assistance in the conduct of privacy impact assessments and threat risk assessments by the Partnership.		
25.	12. Law.	Laws of Ontario and the exclusive forum of Ontario courts to apply. Either party can terminate for cause without the obligation to engage in dispute resolution, mediation or arbitration.		
26.	13. Management and Reporting.	There is to be a process to facilitate rapid notice of failure to conform to the SLAs and to the other terms of the Definitive Agreement and to discuss and resolve such failures.		
27.	14. Payments.	The Partnership may withhold payments on deliverables that are not satisfactorily performed, and payments shall be made on the basis of mutually agreed milestones and not on the mere passage of time.		
28.	15. Proposal Documentation.	At the Partnership's request, all proposal documentation presented by the Supplier, to the extent still applicable to the value proposition proposed by the Supplier, shall be incorporated into the Definitive Agreement.		
29.	16. No Indemnity.	The Supplier will not be seeking an indemnity from the Partnership.		
30.	17. Indemnity from Supplier.	The Supplier shall provide an indemnity, and have in place appropriate insurance, for injury or death to persons or damage to tangible or real property resulting from the negligence of Supplier or product liability claims respecting the IT Solution. The Supplier acknowledges that it, he or she, is not an employee, servant or agent of the Partnership or the Minister and will not represent or hold itself, himself or herself, out to		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		third parties in that capacity. To the extent that any third party, in reliance upon representations by the Supplier, considers the Supplier to be an agent or employee of the Partnership, the Supplier indemnifies the Partnership for any loss or damages and costs occasioned thereby by such third party.		
31.	18. Audit.	During the term of the Definitive Agreement and for two (2) years after the expiration or termination of the Definitive Agreement, the Partnership shall have the right, but not the obligation, to perform financial and security audits of the selected Supplier in relation to the selected Supplier's performance and the invoicing of same.		
32.	19. Recitals.	There shall be detailed recitals that set out the fundamental aspects of the relationship as a part of the Definitive Agreement including the following: a) The funding for this Definitive Agreement provided by the Partnership is, in whole or in part, obtained pursuant to a funding agreement (the "Health Canada Funding Agreement") between the Partnership and Her Majesty the Queen in Right of Canada as represented by the Minister of Health (the "Minister"); b) The Health Canada Funding Agreement requires the Partnership to require certain minimum terms and conditions in agreements; and c) The Supplier acknowledges the source of the funding and recognizes the need to ensure that there is a high level of accountability and transparency in the receipt and expenditure of the funding.		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
33.	20. Force Majeure.	There will be a provision excusing performance for events beyond the reasonable control of a party applying reasonable foresight and due diligence provided: (i) prompt notice is provided of the event; (ii) a workaround strategy is promptly developed; and (ii) all commercially reasonable efforts are used to provide a work-around and to otherwise resume service to the applicable standard. A failure by a subcontractor or agent to perform shall not be an event of force majeure for a party, unless the subcontractor or agent has itself experienced an event of force majeure. Labour disputes or lock-outs suffered or caused by a Party or its subcontractors or agents shall not be considered an event of force majeure. A requirement to disclose Personal Health Information other than under Canadian law pursuant to the terms of this Agreement shall not be an event of force majeure. The application of the force majeure provision shall be limited to 30 days.		
34.	21. Escrow.	The Supplier will agree to a technology materials trust agreement for pre-existing materials. This agreement will permit access to and use of the Supplier's source code and other materials for the IT Solution. Such materials would be held by a third party trustee in Ontario. The materials would include those materials reasonably required to allow the Partnership to independently maintain and support the IT Solution. Release of the materials by the trustee would be triggered by the Supplier's failure to cure a material breach of its Solution-related maintenance obligations or to otherwise make maintenance and support services available.		
35.	22. Novation.	On a minimum of sixty (60) days' prior written notice describing the particulars thereof, the Partnership shall have the right to novate its		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		respective rights and obligations to a new corporation or other entity created to operate the IT Solution.		
36.	23. Appropriation.	Payment under the Definitive Agreement at any given time is subject to the Partnership having been provided funding from the Minister of Health for the service for the fiscal year in which payment is due		
37.	24. Conflict of Interest.	Supplier declares that it has no interest in the business of any third party that would cause a conflict of interest or seem to cause a conflict of interest in performing the IT Solution. Should such an interest be acquired during the term of the Definitive Agreement, Supplier shall declare it immediately to the Partnership. It is a term of the Definitive Agreement that no individual, for whom the post-employment provisions of the Conflict of Interest and Post-Employment Code for Public Office Holders or the Conflict of Interest and Post-Employment Code for the Public Service apply, shall derive a direct benefit from the Definitive Agreement unless that individual is in compliance with the applicable post-employment provisions.		
38.	25. Incapacity to Contract.	Supplier certifies that it and its officers, agents and employees are not prohibited under subsection 750(3) of the Criminal Code from benefiting from a government contract.		
39.	26. Members of the House of Commons.	No member of the House of Commons or the Senate shall be admitted to any share or part of the Definitive Agreement or to any benefit to arise therefrom.		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
40.	27. No Bribe.	Supplier represents and covenants that no bribe, gift, or other inducement has been or will be paid, given, promised or offered directly or indirectly to any official or employee of the Partnership or to a member of the family of such a person, with a view to influencing the entry into the Definitive Agreement or the administration of the Definitive Agreement.		
41.	28. Proactive Disclosure.	Information contained in the Definitive Agreement in relation to the following data elements – proponent name, reference number, effective date, description of the IT Solution, term of the Definitive Agreement, and total Definitive Agreement value may be gathered and may be posted to the Partnership's website. Information that would normally withheld under the *Access to Information Act* and *Privacy Act* will not appear on the website. This public disclosure is intended to ensure that the Definitive Agreement information is collected and presented in a manner that promotes transparency and facilitates public access.		
42.	29. Accounts and Audits.	a) In addition to Section 18 (Audit), the Supplier shall keep proper accounts and records of the cost to the Supplier of the IT Solution and of all expenditures or commitments made by the Supplier in connection therewith, and shall keep all invoices, receipts and vouchers relating thereto. The Supplier shall not, without the prior written consent of the Partnership, dispose of any such accounts, records, invoices, receipts or vouchers until the expiration of six (6) years after final payment under this Definitive Agreement, or until the settlement of all outstanding claims and disputes, whichever is later. b) All such accounts and records as well as any invoices, receipts and vouchers shall at all times during the retention period referred to		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		in sub-section a) be open to audit, inspection and examination by the authorized representatives of the Partnership, the Minister or the Auditor General of Canada, who may make copies and take extracts thereof. The Supplier shall provide all facilities for such audits and inspections and shall furnish all such information as the representatives of the Partnership may from time to time require with respect to such accounts, records, invoices, receipts and vouchers.		
43.	30. Changes.	a) If, on the basis of progress reports provided to the Partnership or for any other reason, the Partnership and the Supplier decide that modifications to the IT Solution or modifications to line items within the budget are needed, the appropriate changes may be made by the administrative contact for the Partnership and the Supplier provided that no increase shall be made to the maximum amount payable hereunder and further provided that no other term of the Definitive Agreement may be altered in this fashion. b) If the change is greater than 15% or $50,000 of the maximum amount payable, whichever is lesser, or if the maximum amount payable changes, the formal addendum process, signed by the approved delegated authority, shall apply.		
44.	31. Communications.	a) In the event that the Definitive Agreement requires work with members of the public, the Supplier shall take the necessary measures to respect the spirit and intent of the Official Languages		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
		Act to communicate with the public in the official language (i.e., English or French) of their choice; b) Any person, including individual researchers, related to the Supplier shall ensure that, as appropriate, announcements, services, documents, conferences, meetings, workshops, etc., be in both official languages, that community members of both official languages be encouraged to participate in its activities, projects or programs and that its activities, projects or programs will meet the needs of the two linguistic communities.		
45.	B. Pricing and Payment Milestones			
46.	(a) Pricing and Price Milestones.	The pricing and price milestones in Exhibit XX [not included] shall apply. No term of the Definitive Agreement or this Letter of Agreement - Term Sheet (LOA-TS) (including this Letter of Agreement - Term Sheet (LOA-TS)) shall be interpreted or applied in a manner inconsistent with the BPS Expense Directive, which directive shall be paramount in all circumstances, with respect to the reimbursement of expenses to Supplier.		
47.	C. Specific Terms Respecting Enterprise HIS Solution			
48.	(a) Integration Specifics.	[To be addressed in negotiations]		

Item No.		SCHEDULE "A" LETTER OF AGREEEMENT - TERM SHEET (LOA-TS)	Response	Exceptions
49.	2. Network Availability.	[To be addressed in negotiations]		
50.	3. Technical Requirements	[To be addressed in negotiations]		
51.	4. Hosting Services.	Among other provisions, if the Supplier is providing Hosting Services, it agrees to conform to the security provisions in Schedule "D".		

Item No.		SCHEDULE "B" UPTIME AND RESPONSE TIME REQUIREMENTS	Response	Exceptions
52.		**[NTD: To be consistent with supplier's response to the RFP SLAs.]**		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
53.	**Definitions and Interpretation**			
54.	**1.**	In this Schedule, the following terms have the following meanings and any capitalized terms that are not defined in this Schedule "C" have the meaning attributed to them in the Agreement:		
55.		a) "access" in connection with Personal Data, means to have access whether or not the Personal Data is actually read, reviewed, scanned, copied or otherwise used;		
56.		b) "Authorized Personnel" has the meaning attributed thereto in section 8(c) below;		
57.		c) "Contact Information" means the name of a person (when used in his or her capacity as an employee, independent contractor, officer or director of the Partnership) and the person's position or title, business address, business telephone number, and any other information that is from time to time excluded from the definition of "personal information" in the *Personal Information Protection and Electronic Documents Act* (Canada);		
58.		d) "Supplier Privacy Requirements" means the obligations of and the restrictions and prohibitions applicable to the Supplier in regard to Personal Data set out in this Schedule "C" and in any privacy law applicable to Supplier in its capacity as a service provider to the Partnership;		
59.		e) "Personal Data" means collectively, "Personal Information" and "Personal Health Information";		
60.		f) "Personal Health Information" means information to which Supplier has access as a function of providing the IT Solution that identifies an individual and relates to: his or her physical or mental health, including the health history of the individual's family; the providing of health care to the individual, including the identity of his or her health care providers, substitute decision-		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
		makers and health numbers; payments or eligibility for health care or health care coverage; and the donation of a body part or bodily substance, or the testing or examination thereof;		
61.		g) "Personal Information" means information to which Supplier has access as a function of providing the Hosted and Services Solution that identifies an individual, but does not include Contact Information; and		
62.		h) "use" in connection with Personal Data means to handle Personal Data in any manner, including to copy, download and hold Personal Data, but excludes the de-identification of Personal Data.		
63.	2.	References to Supplier include its employees and agents, including permitted subcontractors, unless otherwise provided.		
64.	**Relationship of the Parties**			
65.	3.	The Partnership is the provider of Cancer View Canada, an Internet-based portal environment that among other services provides electronic means for individuals to collect, use, disclose and retain Personal Data and also operates certain back office systems containing Personal Data applicable to its operations.		
66.	4.	Supplier is a service provider retained under this Agreement to assist the Partnership in connection with Cancer View Canada by providing the IT Solution.		
67.	5.	Supplier is responsible for the acts and omissions of Authorized Personnel in regard to Personal Data.		
68.	6.	Nothing in this Agreement will be construed to grant Supplier any custody, control, title or rights or interest in or to Personal Data.		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
69.	**Restricted Use of Personal Data**			
70.	7.	Supplier acknowledges and agrees that it will be necessary for Supplier to access, use, hold, store and transfer Personal Data to provide the IT Solution.		
71.	8.	In providing the IT Solution, Supplier will comply with the Supplier Privacy Requirements and without limiting the generality of the preceding, Supplier will:		
72.		(a) only access and use Personal Data as necessary to provide the IT Solution and will not access or use Personal Data for any other purpose or on its own behalf;		
73.		(b) not disclose Personal Data to any person or organization including without limitation, to an affiliated third party;		
74.		(c) not permit its employees or any person acting on its behalf ("Authorized Personnel") to have access to Personal Data unless such access is required for Supplier to provide the IT Solution and unless Authorized Personnel agree to comply with all applicable Supplier Privacy Requirements.		
75.	9.	For clarity, the access and use of Personal Data under this Schedule "C" by Authorized Personnel does not constitute a disclosure of such Personal Data by Supplier to Supplier Authorized Personnel.		
76.	10.	Supplier acknowledges that information which is Confidential Information, as defined in the Agreement, may also be, but is not necessarily, Personal Data. Where information is Confidential Information and Personal Data, the requirements applicable to each type of information will apply to so as to subject the information in each case to the more rigorous requirement.		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
77.	11.	If Supplier receives any request for access to or the correction of Personal Data which it is holding or storing to provide the IT Solution, Supplier will promptly direct the request to the Partnership, provided, however, that nothing in this Schedule "C" will be interpreted or construed to prohibit Supplier from complying with any valid court order made under the laws of Ontario or the laws of Canada applicable in Ontario (but for clarity, not an order made under the laws of any other jurisdiction), on written notice to the Partnership.		
78.	**Protection of Personal Data**			
79.	12.	Any Personal Data held by Supplier for the purpose of providing the IT Solution will be held in a secure physical and electronic environment in Ontario meeting or exceeding the standards relating to the protection of sensitive personal information set out in this Schedule.		
80.	13.	Except with the prior written authorization of the Partnership, Supplier will not transfer or permit access to Personal Data to any person, including Authorized Personnel, or facility outside of Ontario.		
81.	14.	To the extent that Supplier holds Personal Data, Supplier will not comingle Personal Data with any other data.		
82.	15.	Supplier will maintain a record of access to the Partnership data, by Authorized Personnel or by any person from equipment controlled by Supplier, which record will include the identity of the person who accessed the Partnership data, the date and time of access and the duration of the session. Supplier will produce such record to the Partnership at its request and retain such record for a minimum of seven (7) years from the date on which the Agreement expires or terminates.		
83.	16.	If the Partnership determines, in its sole discretion, that a practice or procedure used by Supplier to provide the IT Solution would violate a privacy requirement applicable to the Partnership, as a result of a legislative change, a finding, order or decision of a regulatory authority with jurisdiction over Personal Data, or for any other reason, the Partnership may		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
		amend this Agreement to vary or eliminate such practice or procedure on prior written notice to Supplier, subject to the Change Order Process in the Agreement.		
84.	17.	Supplier will promptly advise the Partnership if it believes that any practice or procedure in which it is engaging in connection with the IT Solution contravenes a privacy requirement, or if it receives or learns of any complaint or allegation to that effect.		
85.	18.	Supplier will use safeguards and meet a standard of protection that are appropriate for protecting sensitive information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal.		
86.	19.	Without limiting the generality of section 8(c) above, Supplier will:		
87.		a) ensure that Authorized Personnel receive sufficient training to be able to comply with the applicable Supplier Privacy Requirements;		
88.		b) take reasonable steps, through means such as training, confidentiality agreements and the application of appropriate sanctions, to ensure Authorized Personnel comply with applicable Supplier Privacy Requirements;		
89.		c) ensure that immediately upon termination or expiry of their employment by or affiliation with Supplier, access of Authorized Personnel to Personal Data is terminated and any and all Personal Data being held by Authorized Personnel is left with Supplier;		
90.		d) terminate access of Authorized Personnel to Personal Data and replace Authorized Personnel where the acts or omissions of Authorized Personnel are reasonably likely to threaten the security and/or integrity of Personal Data or Supplier's compliance with the Supplier Privacy Requirements, and on the reasonable request of the Partnership; and		
91.		e) not permit staff of any permitted subcontractor access to Personal Data unless and until such subcontractor has signed a written		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
		agreement requiring it to comply with applicable Supplier Privacy Requirements, including agreeing to the inspection and audit described in Section 23 of this Schedule "C" and permitting Supplier to terminate its agreement with such subcontractor where its acts or omissions are reasonably likely to threaten Supplier's compliance with the Supplier Privacy Requirements.		
92.	20.	Supplier will co-operate with the Partnership, acting reasonably, where the Partnership requires Supplier's assistance in regard to:		
93.		a) security or privacy events, including without limitation any breach, that could reasonably threat or threatens the security and/or integrity of Personal Data;		
94.		b) inquiries, complaints, or investigations relating to Personal Data;		
95.		c) assessments being conducted by or on behalf of the Partnership, including privacy impact and threat risk assessments, that involve the IT Solution.		
96.	21.	Supplier will notify the Partnership:		
97.		a) promptly, of any inquiries, complaints or investigations referred to in section 20(b) above;		
98.		b) promptly, if it determines that, for any reason, it does not or will not be able to comply with this Schedule "C", outlining the particulars and the steps Supplier proposed to take to address the non-compliance or prevent the anticipated non-compliance; and		
99.		c) notwithstanding paragraph (b) above, immediately upon becoming aware of the theft, loss, or unauthorized access, use, modification,		

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
		disclosure or destruction of Personal Data or where there is a reasonable likelihood that such an event could have occurred.		
100.		Notwithstanding anything to the contrary in the Agreement, the Partnership may:		
101.		a) make application for a court order preventing or terminating any non-compliance by Supplier with this Schedule "C"; and		
102.		b) terminate the Agreement on notice in the event that the Partnership determines that Supplier has breached this Schedule "C", and Supplier has failed to cure the breach in accordance with Section 9.2 of the Agreement.		
103.	**Audit, Inspection**			
104.	23.	In addition to the audit described in the Agreement, the Partnership or an independent auditor retained by the Partnership for the purpose that has entered into a mutually acceptable confidentiality agreement with the parties, will have the right, during normal business hours and upon reasonable notice to Supplier, to visit and inspect all locations at which Supplier, or any of its permitted subcontractors, accesses, uses, holds or stores Personal Data, to examine all equipment used, and all records in connection therewith, to make copies of such records and to ask questions of Authorized Personnel (including permitted subcontractors) reasonably required to verify Supplier's compliance with this Schedule "C" and otherwise to audit and verify, both physically and electronically, compliance by Supplier with this Schedule "C". Notwithstanding the preceding, the Partnership will have no duty to make any such visit, inspection, examination, audit or verification and will not incur any liability or obligation by reason of doing or not doing so.		
105.	**Termination and Survival**			

Item No.		SCHEDULE C PROPOSED LETTER OF AGREEMENT – TERM SHEET (LOA-TS) PRIVACY PROVISIONS	Response	Exceptions
106.	24.	Notwithstanding [section 8.6] of the Agreement, in the event of the termination or expiry of this Agreement, or at any other time at the Partnership's request in respect of some or all Personal Data, Supplier will forthwith at the Partnership's discretion, securely return to the Partnership or securely destroy all Personal Information held by Supplier pursuant to this Agreement without retaining any copies, excluding archival or long term back up storage that is not exclusive to Personal Data. Upon request, an officer's certificate attesting that such actions have been completed and that there are no tangible and/or available electronic versions of Personal Data being held by Supplier will be provided to the Partnership by Supplier, except for archival or long term back up storage that is not exclusive to Personal Data. Supplier undertakes not to recreate, in whole or in part, any copy of Personal Data (including, but not limited to an electronic copy) at any time after the return or destruction of Personal Data. Where commercially reasonable to do so or as otherwise provided for in this Agreement, Supplier will apply procedures to segregate the Partnership data from other data sources. Supplier shall share its data destruction policy with the Partnership in relation to data that may be co-mingled with the Partnership data.		
107.	25.	Notwithstanding the termination of the Agreement, to the extent that Supplier continues to have access to Personal Data for any reason, Supplier will continue to govern itself in accordance with the terms of this Schedule "C".		
108.	26.	The obligations of Supplier under this Schedule "C", regarding ownership and control of Personal Information, access, use and non-disclosure of Personal Data and Authorized Personnel's compliance with such provisions, will survive the termination of the Agreement.		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
109.	**1. SECURITY**			
110.		The Parties acknowledge the fundamental importance of establishing logical and physical controls in order to maintain the security, integrity and availability of the IT Solution, and limit unauthorized access, destruction, loss or alteration to, and disclosure of, the Partnership's Confidential Information and any Personal Information, in all formats including but not limited to electronic and paper formats in accordance with this Agreement. As such, Supplier agrees to establish and maintain and to ensure each of its subcontractors establish and maintain minimum safeguards as defined below:		
111.		(a) Information Security Policy and Procedures. Establish and maintain formal information security policies and procedures establishing controls around the Partnership's Confidential Information and Personal Information, and the systems that process them, in accordance with the requirements of the Partnership.		
112.		(b) Information Security Organization. Define responsibility for the ongoing review of		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
		information security safeguards to reasonably ensure its continuing suitability, adequacy and effectiveness, in accordance with the requirements of the Partnership, and changing threats to security.		
113.		(c) Asset Management. Define the inventory of data centre, facilities and systems that create, store, process and disseminate the Partnership's Confidential Information and Personal Information, and establish ownership and responsibility for the successful operation of security controls for each of those environments.		
114.		(d) Human Resources. Establish and maintain controls to ensure that employees, contractors and third party staff are suitably screened and educated on security practices prior to being given access to the Partnership's data and the systems that process that data, and that all individual access to the Partnership's Confidential Information and Personal Information, is promptly removed upon termination of employment, agreement or contract with Supplier, or adjusted upon a change in role. At the request of the		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
		Partnership, Supplier will be obligated to provide a list of individuals that have access to IT resources related to the Partnership.		
115.		(e) Physical and Environmental Security. Establish a security perimeter around the physical work environment and sensitive data processing facilities, and establish physical entry controls to reasonably ensure that only authorized individuals gain access to the environment, and environmental controls to protect against damage from fire, flood, and other forms of man-made or natural disasters.		
116.		(f) Communications and Operations Management. Establish operating procedures and controls for the secure operations of systems and networks facilitating the access to the Partnership's Confidential Information and Personal Information in order to reasonably prevent accidental or deliberate misuse. Such controls include, but are not limited to, change management, least privileges granted, segregation of duties, separation of production environment from development/test environments, backups, network security, and the encryption of media in transit between the		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
		Partnership and Supplier. In addition, Supplier will maintain a secure communication link (e-mail, telephony, etc.) to ensure that Confidential Information and Personal Information travelling between the two parties remains secure.		
117.		(g) Access Controls. Establish controls and procedures for the authorization, regular review and revocation of access at all levels of the system environment including physical access, network access, operating systems, applications and database access. Maintain suitable authentication controls to reasonably ensure that an individual's access rights to the Partnership's Confidential Information and Personal Information is appropriate for the individual's role regardless of how that individual is attempting to access that information or the location from which access is being attempted.		
118.		(h) Information Systems Acquisition, Development and Maintenance. Maintain an application development and maintenance framework that protects the integrity of the production application and associated source code from		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
		unauthorized and untested modifications. Such a framework shall establish control over the Partnership's Confidential Information and Personal Information, across all environments within the development lifecycle of systems.		
119.		(i) Incident Management. Establish policies and procedures for the timely communication and investigation of suspected breaches in the security of the Partnership's Confidential Information and Personal Information. At a minimum, communication of such incidents to the Partnership must take place prior to any discussion with regulators, clients, outside law enforcement agencies or representatives of the media. Incident investigations and associated information handling shall be performed in accordance with Applicable Law.		
120.		(j) Business Continuity Management. Establish appropriate policies and procedures to ensure continued provision of Services in accordance with timelines defined by the Parties as part of the Transition Services.		
121.		(k) Compliance. Establish policies and procedures to ensure that the design, operation and		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
		management of systems controlled by Supplier or its Subcontractors and processing the Partnership's Confidential Information and Personal Information meets the requirements of Applicable Law, and the requirements established in this Agreement.		
122.		(l) Data Destruction and Disposal. Supplier will implement processes and controls to ensure that any storage media or data is disposed or destroyed securely in accordance to the requirement of the Partnership.		
123.		(m) Auditing: Supplier will maintain wherever possible an audit trail of the associated activities by staff or automated processes. Supplier will make available upon the Partnership's request any reports related to specific actions.		
124.		(n) Review: Supplier shall conduct regular control reviews of security of the Services, including, as applicable, penetration testing and intrusion detection, malware alerts, and share the results of such reviews with the Partnership.		

Item No.		SCHEDULE D Proposed Letter of Agreement – Term Sheet (LOA-TS) Security Provisions	Response	Exceptions
125.	**2. VERIFICATION AND AUDIT OF SECURITY COMPLIANCE.**	Supplier represents and warrants that it maintains adequate internal audit functions to assess internal controls in its environment, and to protect the security and confidentiality of any of the Partnership's Confidential Information and Personal Information which will be confirmed by the audit report referred to in the herein. Supplier agrees to provide documentation regarding its internal controls to the Partnership upon request. Upon the Partnership's request, Supplier will provide at the Partnership's expense a report of an independent, reputable, audit firm, which report shall be compliant with the Canadian Standard on Assurance Engagements (CSAE) 3416 Reporting on Controls at a Service Organization, as such standard may be superseded, amended or replaced from time-to-time. Each report shall cover the Services and the IT Solution for a consecutive twelve (12) month period ending March 31 in each year during the term of this Agreement. Supplier shall provide the Partnership with a copy of each report within thirty (30) Business Days following its receipt.		

APPENDIX B – Form of Offer

The Proponent must not amend this Form in any way other than by providing the requested information. This form must be completed, signed and submitted as part of the Proponent's Proposal.

To the Canadian Partnership Against Cancer:

1. Proponent Information

(a) The full legal name of the Proponent is:

_____

(b) Any other registered business name under which the Proponent carries on business is:

_____

(c) The jurisdiction under which the Proponent is formed is:

_____

(d) The name, address, telephone, facsimile number and e-mail address of the contact person for the Proponent is:

_____

(e) Indicate whether the Proponent is an individual, a sole proprietorship, a corporation or a partnership:

_____

2. Offer

The Proponent has carefully examined the RFP documents and has a clear and comprehensive knowledge of the IT Solution required under the RFP. By submitting the Proposal, the Proponent agrees and consents to the terms, conditions and provisions of the RFP, including the Term Sheet set out in Appendix A of the RFP, and offers to provide the IT Solution in accordance therewith at the price set out in the Rate Bid Form at Appendix C.

3. Price

The Proponent has submitted its price in accordance with the instructions in the RFP and in the form set out at Appendix C.

4. Conflict of Interest

The Proponent, by submitting the Proposal, confirms that to its best knowledge and belief no actual or potential Conflict of Interest exists with respect to the submission of the Proposal or performance of the contemplated Agreement other than those disclosed in this Form of Offer. Where the Partnership discovers a Proponent's failure to disclose all actual or potential Conflicts of Interest, the Partnership may disqualify the Proponent or terminate any Agreement awarded to that Proponent as a result of this procurement process.

Conflict of Interest includes, but is not limited to, any situation or circumstance where:

a) in relation to the RFP process, the Proponent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to
    i. having or having access to information in the preparation of its Proposal that is confidential to the Partnership and not available to other Proponents;
    ii. communicating with any person with a view to influencing preferred treatment in the RFP process; or
    iii. engaging in conduct that compromises or could be seen to compromise the integrity of the RFP process and render that process non-competitive and unfair; or
b) in relation to the performance of its contractual obligations under the Agreement, the supplier's other commitments, relationships or financial interests
    i. could or could be seen to exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgment; or
    ii. could or could be seen to compromise, impair or be incompatible with the effective performance of its contractual obligations;

Proponents must choose one of the following two options.

☐ The Proponent declares that: (1) there was no Conflict of Interest in preparing its Proposal; and (2) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFP.

OR

☐ The Proponent declares that there is an actual or potential Conflict of Interest relating to the preparation of its Proposal, and/or the Proponent foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFP. The details of the actual or potential Conflict of Interest are as follows:

5. Disclosure of Information

The Proponent hereby agrees that any information provided in this Proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or if required by order of a court or tribunal. The Proponent hereby consents to the disclosure, on a confidential basis, of this Proposal by the Partnership to its advisers retained for the purpose of evaluating or participating in the evaluation of this Proposal.

6. Execution of Agreement

The Proponent understands that, in the event its Proposal is selected by the Partnership, in whole or in part, the Proponent agrees to finalize and execute an Agreement incorporating the terms and conditions set out in Appendix A to the RFP, in accordance with the terms of the RFP.

7. Limitation of Liability

The Proponent acknowledges and agrees that the Partnership shall have no liability to Proponent or its sub-contractors in respect of the conduct of the procurement process relating to this RFP by the Partnership, whether in contract or tort or otherwise, and including, without limitation, for costs that the Proponent or its sub-contractors incur with respect to the procurement process or for any loss of profit the Proponent or its sub-contractors incur as a result of not being awarded a contract under this procurement process. The limitation of liability shall apply whether or not based on an allegation, whether in whole or in part, true or not, that the Partnership has conducted an unfair procurement process.

8. Paramountcy

The Proponent acknowledges and agrees that this Form of Offer is paramount in the event of any inconsistency or conflict with any other aspect of Proponent's Proposal.

Signature of Proponent representative:

Name and Title of Proponent representative:

Date:

I have authority to bind the Proponent.

APPENDIX C – Rate Bid Form

Total Fees From January 2017 to March 31, 2022*(000's)*					
Component	Transition Project Work			On-going Support	Total
	Jan-17	Feb-17	Mar-17	Apr. 1, 2017 to Mar. 31, 2022	
Infrastructure Build					
Planning & Design					
Implementation & Configuration					
Hardware & Support					
Service Desk					
Planning & Design					
Implementation & Configuration					
Software & Support					
On-Going Operations					
Managed Hosting					
Planning & Design					
Implementation & Configuration					
Software & Support					
On-Going Operations					
Application Management					
Planning & Design					
Implementation & Configuration					
On-Going Operations					
Sub-Total					
HST					
Total					

Total On-Going Support Fees by Fiscal Year*(000's)*						
	April 1, 2017 to March 31, 2018	April 1, 2018 to March 31, 2019	April 1, 2019 to March 31, 2020	April 1, 2020 to March 31, 2021	April 1, 2021 to March 31, 2022	Total
Service Desk						
Application Management						
Managed Hosting						
Hardware & Support						
Service Desk - Software & Support						
Sub- Total						
HST						
Total						

Please note that the positions listed below are sample listings and the Proponent are encouraged to add the positions required to support the IT Solution.

Please answer the following questions.	YES / NO
Does your company use off-shore resources for support and implementation?	*Yes/No*
Will you use off-shore resources for support and implementation of the proposed Solution for GRHC, if your Solution becomes the winning bid?	*Yes/No*

Role - Local or North America (please specify)	Hourly Rate (CAD) (Local / North America)	Hourly Rate (CAD) (Off-Shore - where available)	Average Rate per Resource
Project Manager			$
Technical Lead			$
Project Analyst			$
Technical Analyst			$
Report Analyst			$
Training Specialist			$
** Please include additional roles applicable to proposed solution. (*add rows if required*)			

The Rate Card should be fixed for the first three years of the contract, after which provision for inflationary percentage increase should be included. Please identify the maximum percentage increase for each of years 4 - 5 in the table below.

Year of Contract	Maximum % increase
Year 4	
Year 5	

APPENDIX D – Client Reference Form

The Proponent **should** provide a completed Client Reference Form as follows:

- One (1) reference where the Proponent has had a long-term (> 5 years) relationship for IT Support Services.
- Two (2) references for Microsoft Azure Cloud Managed Services
- Two (2) references for IT Service Desk Services

Proponent: _____

Reference #1 –Long Term Relationship

Company Name:	
Company Address:	
Contact Name:	
Contact Title:	
Contact Telephone Number:	
Date Work Undertaken:	
Nature of Assignment:	

Reference #2 – Microsoft Azure Cloud Managed Services

Company Name:	
Company Address:	
Contact Name:	
Contact Title:	
Contact Telephone Number:	
Date Work Undertaken:	
Nature of Assignment:	

Reference #3 - Microsoft Azure Cloud Managed Services

Company Name:	
Company Address:	
Contact Name:	
Contact Title:	
Contact Telephone Number:	
Date Work Undertaken:	

Nature of Assignment:	

Reference #4- IT Service Desk Services

Company Name:	
Company Address:	
Contact Name:	
Contact Title:	
Contact Telephone Number:	
Date Work Undertaken:	
Nature of Assignment:	

Reference #5 - IT Service Desk Services

Company Name:	
Company Address:	
Contact Name:	
Contact Title:	
Contact Telephone Number:	
Date Work Undertaken:	
Nature of Assignment:	

EXHIBIT A - Current State & Future State Information

This Exhibit outlines the Partnership's current state information related to its IT services and infrastructure and also includes current thinking for a future state hybrid cloud environment and five year growth projections for key metrics. Proponents should use the information in this section as a reference in completing their Proposal.

Current State Information

- User Profile/Service Desk Usage
- Digital Properties
- IT Service Catalogues
    - Tier 1
    - Tier 2
    - Tier 3 (Vendor Management)
- IT Infrastructure: Current State
    - Overview
        - General network architecture diagram
        - Disaster Recovery
    - Environment: Peer 1 Toronto East (Production)
        - Physical infrastructure
        - Server and application inventory
    - Environment: Peer 1 Toronto II, 151 Front St.(Development, Staging, Disaster Recovery)
        - Physical infrastructure
        - Server and application inventory
    - Environment: SAAS
        - Pagely
        - Igloo
    - vSphere Capacity Report
- Hardware Inventory for One University Ave. Office
- Software Inventory for One University Ave. Office
- Standard Operating Procedures (SOPs)
- Corporate Information Systems Diagram
- Privacy and Security Framework
- Information Technology Team Organization

Future State Information

- IT Infrastructure: Future State
- Future Hybrid Cloud Configuration
- 5-year Growth Projections for Key Metrics

Current State Information

User Profile/Service Desk Usage

- The Partnership has an average volume of 160 Service Desk incidents per month
    - Average volume of 90 Service Desk calls per month
    - After hours calls are rare and average once a month
- The top categories for current volumes include:
    - Identity and Access
    - Informational (providing users information)
    - PCs
    - MS Outlook
    - Wireless
    - Remote Access
- Partnership users have a medium level of technical proficiency
- Most end users external to the Partnership are very busy and have little time to deal with problem resolution

Digital Properties

Property	Internal or External
http://www.partnershipagainstcancer.ca/	External
http://www.cancerview.ca/	External
http://blog.cancerview.ca/	External
http://www.canadiancancertrials.ca/	External
http://www.systemperformance.ca/	External
http://www.partnershipfortomorrow.ca/	External
http://www.yourcancerstory.ca/	External
https://analyticallyyours.mycancerview.ca/	Internal + External
https://hub.cancerview.ca/ + 28 other community sites	Internal + External
https://centralperk.cpacc.ca	Internal
http://www.virtualhospice.ca/ (Hosting only)	External
http://crmm.cancerview.ca/cpacmodgenweb/	External
https://elearning.cancerview.ca/moodle/	Internal + External

IT Service Catalogue – Tier 1

Service	How to Request
Employee Changes	
Onboarding of new employees	Onboarding Form

• Setting up standard hardware including laptops, monitors, keyboards, mice, docking stations, and phones in a staff member's office space. • Setting up standard software, non-standard software, email accounts, and network access. • Ensuring correct access to corporate IT services and applications.	
Off boarding employees • Removing software • Removing accounts and access • Receiving returned employee's hardware	Off boarding Form
Role changes for employees • Updating accounts, access, and role change information.	Role Change Form
Software	
Standard Software • Setting up and supporting standard software issues	Email Service Desk
Optional/Department-specific software • Setting up software because of specialized needs	Email Service Desk
New Software • Setting up new software that is not considered standard software at the Partnership • Requests are subject to review and approval by IT and other parties for reasons of cost, compatibility, and security.	IT Request Form
Access, Permissions and Settings	
Records Management access • Creating 1st, 2nd, or 3rd level folders • Creating confidential folders • Granting access to confidential folders	RM Request Form
Email/calendar access and permissions • Granting access to another user's email or calendar in Outlook	IT Request Form
Central PERK Intranet permissions • Adding user as a Content Editor • Adding user as Space Creator	IT Request Form
Meeting room calendars • Granting access to meeting room calendars	Email Service Desk
Email distribution lists • Adding or removing users from Outlook distribution lists	Email Service Desk
Hardware	
Work from home setup • Providing hardware including docking station, keyboard, monitor, mouse, and USB headset for staff to take home.	IT Request Form

Computer support • Connecting to the network/wireless • Troubleshooting hardware issues • Replacing defective computers	Email Service Desk
Mobile phone provisioning • Setting up and supporting the Partnership's mobile devices and their email, calendar, and corporate apps. This also applies to personal mobile devices used as Bring Your Own Device. • Replacing defective mobile devices and transferring of corporate data	Email Service Desk

Phone support and features
• Replacing defective desk phones, headsets, Polycom conference phones.
• Supporting hardware issues
• Adding or removing phone features
  ○ Mobile connect
  ○ Unified messaging
  ○ Soft phone (IP Communicator)
	Email Service Desk

Personal printers • Setting up or replacing printers • Connecting printers to the network • Fulfilling toner requests • Supporting basic printer issues	Email Service Desk
Loaner and presentation devices • Providing temporary access to laptops, mobile devices, Rogers LTE Stick, IronKey Secure USB Key.	Email Service Desk
Meetings	
Audio, web and video conferencing • Setting up WebEx accounts and troubleshooting issues • Adding more audio capacity of more than 50 participants on WebEx teleconferences. • Setting up BlueJeans accounts and troubleshooting issues • Supporting Meet Me audio conferencing	Email Service Desk
Meeting room services • Supporting technical issues related to WebEx and Blue Jeans meetings being conducted in meeting rooms • Supporting issues related to meeting room hardware (e.g. touch panel, microphones, projector, screens, and cameras)	Email Service Desk

IT Service Catalogue – Tier 2

Service	How to Request
Acquisition / Procurement Services	
Software Licenses • Purchasing PC software and server plugins	Email Service Desk
SSL Certificates • Purchasing, implementing, reconfiguring, and removing SSL certificates for applications and web servers	Email Service Desk with IT Director authorization
General IT Procurement • Purchasing general IT products • Purchasing Roger's phone and travel packages	Email Service Desk
Development Services	
• Deploying new servers • Creating and initializing virtual hosts/new servers for deployment	IT Director Authorization Email Service Desk
Trial/Pilot New Software/Product Solutions • Researching and investigating new software • Running pilots and demos of new software to potentially deploy • Preparing quotes and being the point of contact for new products/services being evaluated	Email Service Desk
Service Promotion • Migrating services between Development, Staging, and Production environments ○ Typically the actual data move/initial import completed by Service Desk with the Partnership handling the actual configuration of service	IT Director Authorization Email Service Desk
Operations and Support	
Server and Application Updates • Conducting application updates • Conducting operating system upgrades • Installing plugins and its maintenance	Email Service Desk
Network Changes • Altering network routes • Modifying core Firewall rules	Email Service Desk (Requests

• Adding/Editing VIPs	must come from the Partnership's IT Service Leadership)
Domain Name Changes / Reconfiguration • Purchasing and creating DNS records • Editing Public and Private DNS records	Email Service Desk with IT Director authorization
Antivirus (McAfee) Service Management • Modifying Antivirus / Local Firewall Rules • Collecting and analyzing McAfee Security Center Report	Email Service Desk

Network / Server Triage
• Restoring network/service outages. For example:
  ○ Web VPN
  ○ Network routing
  ○ Performance and quality of service issues
• Note that most core services are proactively monitored
	Email or call Service Desk

Application Support Issues / Triage
• Triaging and supporting application issues. For example:
  ○ Files not uploading properly
  ○ Page Errors
  ○ Service not responding
• Initial triage completed by IT Service Vendor before Tier 3 escalation)
	Email or call Service Desk

Phone / Phone System Issues / Triage
• Triaging and supporting phone / phone system issues. For example:
  ○ Phones not connecting to the call system
  ○ Call system not routing calls correctly
  ○ Call outages
  ○ Call quality issues
	Email Service Desk

Privacy and Security • Investigating security incidents	Email Service Desk
Accounts, Access and Permissions	
User Access Permissions • Setting account permissions for services	IT Request Form Email Service Desk
Active Directory Group Membership and Permissions • Adding users to appropriate Active Directory groups • Adjusting permissions for groups, people, files and folders	IT Request Form

	Email Service Desk
File / Group Access Permissions • Setting up and configuring access to network shares, services, and devices	IT Request Form Email Service Desk
Records Management	
Managing Records • Auditing Mimecast records • Restoring records • Looking up email records	IT Request Form (or request must come from IT Director) Email Service Desk
Ticket Reports and Analysis • Auditing ticket logs and open tickets • Analyzing and reporting on survey results	Email Service Desk

IT Service Catalogue – Tier 3 (Vendor Management)

Service	How to Request
Vendor Management / Liaison	
Agresso • Outage / Triage for complete service loss • Feature requests	Email or call Service Desk who will escalate and involve Agresso as required
WebEx/BlueJeans service Outage and Triage • Multiple users unable to create/attend webinar meeting	Email or call Service Desk who will immediately escalate to the Service Provider
CRM2013 Application Support • Application not loading or is crashing with critical errors	Email Service Desk who will involve Vendor Support
Boardroom A/V Equipment Failure • Projector not functioning • Microphones and speakers are not powering up	Email Service Desk to coordinate a site visit if needed
Igloo Software Outage and Triage • Igloo community service outage • Functions are not working correctly • Pages reporting errors • Igloo Desktop software crashes	Email or call Service Desk who will liaise with Igloo Support for service restoration
Empower ID • SSO configuration issues	Email or call Service Desk who will escalate and

• Feature requests • SSO system outage or critical errors	involve Empower ID as required
PRI Circuit (TELUS) Outages • Unable to connect Telus PRI lines	Email Service Desk who will involve Telus as required for onsite visit
EI Circuit Degradation / Outage • Bell EI circuit disconnected or unresponsive	Email or call Service Desk who will escalate and involve Bell as required
Network / Server Equipment Failure • Complete network outage • Symptoms include multiple users unable to access the internet, email, shared drives, or any other network servers	Email or call Service Desk. Note that Service Desk provides proactive monitoring and will be sent an alarm Service Desk will liaise with Cisco to restore
Core Operating System Faults • Linux Kernel Errors • Core System/Kernel reconfiguration	Email Service Desk who will liaison with Red Hat
vSphere Bug / becomes unrecoverable • vSphere Fails to boot • Failover Errors • Software Bugs	Email or call Service Desk who will escalate to VMWare as required

IT Infrastructure: Current State

Overview

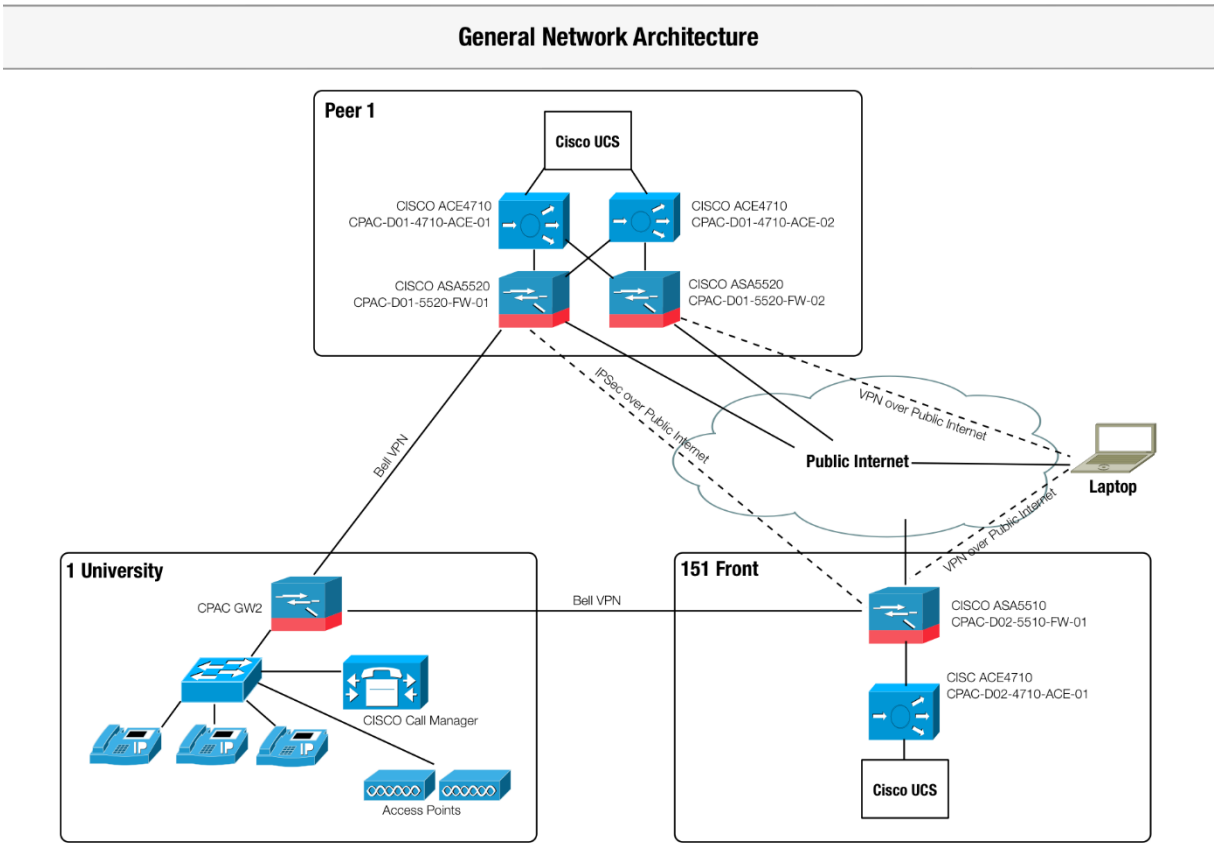
The Partnership's infrastructure is currently co-located in two data centers within the Greater Toronto Area. The primary data center is located at Peer 1 Toronto East in Scarborough and hosts the Partnership's production environment. The secondary data center is located at Peer 1 Downtown II, 151 Front St. in Toronto and hosts the Partnership's development, staging and disaster recovery environments. The Partnership has implemented the Cisco /NetApps FlexPod unified architecture with VMWare to support virtualization and disaster recovery using NetApp SnapMirror /VMware SRM across the two locations. There are approximately 200 active virtual machines (VMs) across the production, staging and development environments.

Over the past two years, the Partnership has been undergoing a technology transformation from a legacy Oracle environment to open source and SaaS based solutions which the Partnership expects to complete in 2016. As a result of these technology transformations, we expect to reduce our VM footprint by approximately 100 active VMs and significantly reduce the complexity of our server and network infrastructure.

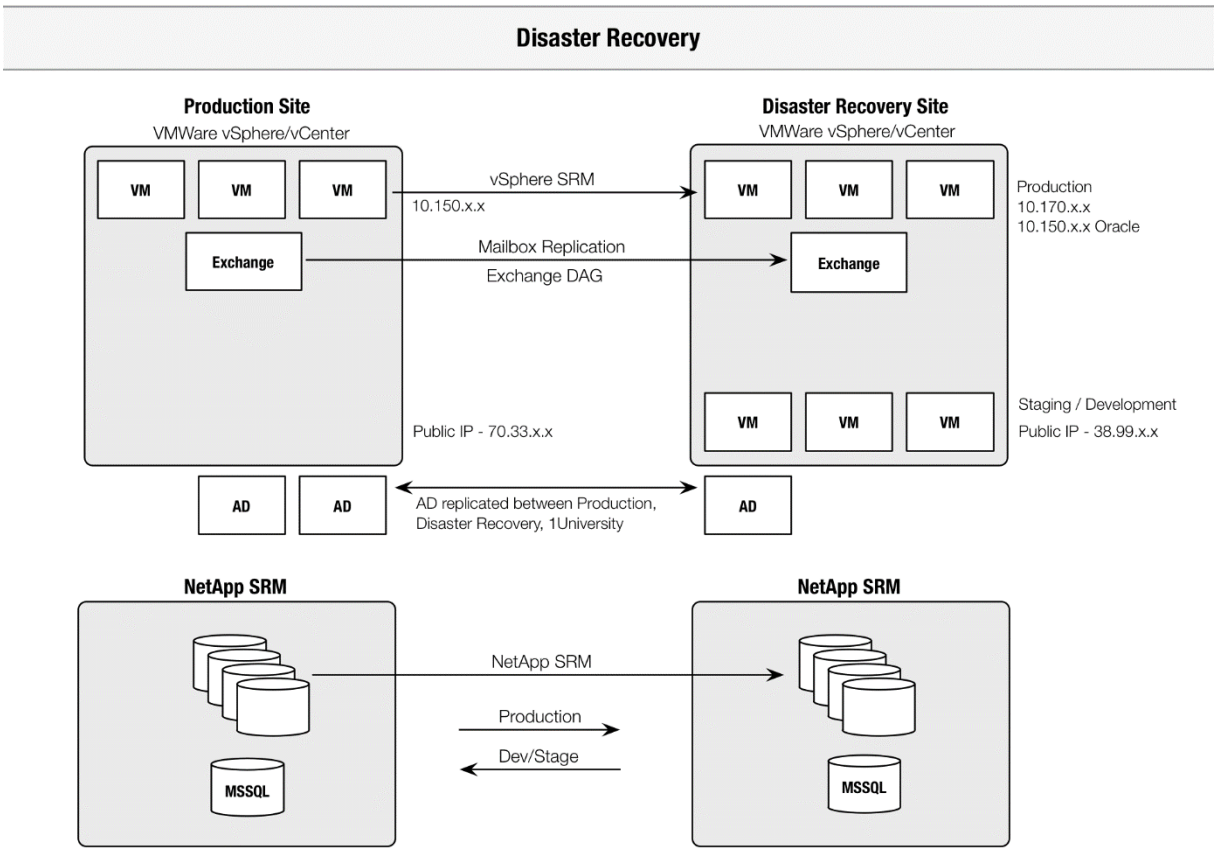
Additional pilots and evaluations are currently in progress (e.g., Office 365 and Skype for Business) which may result in further service transitions to the cloud prior to commencement of the new IT vendor contract and changes to the Tier 3 catalog (above).

These transitions would also result in further reductions in complexity for our managed environments (e.g., retiring Exchange 2010 MBX and CAS servers at both data centres) and scope of responsibilities for the Proponent.

General network architecture diagram



Disaster Recovery



Environment: Peer 1 Toronto East (Production)

Physical Infrastructure: Peer 1 (Production)

General BOM

Cisco Nexus Switching
(2) Nexus 5548UP Chassis each with:
- (1) Layer 3 Daughter Cards
- (4) 10GBase-SR SFPs
- (6) 1000Base-T SFPs
- (4) 8 Gbps FC SFP+
- (1) 8-port Nexus 5500 Licenses
- (1) Nexus 2248TP-E 48 port 1GbE (RM5) remote linecard

(2) Nexus C1010 Appliances (HA Pair)

Cisco Networking Services
(1) Global Site Selector 4492R Appliance
(2) Application Control Engine 4710 Appliance
(2) Adaptive Security Appliance 5529 with:
- (1) AIP-SSM-20 IPS/IDS Daughter Card

NetApp Storage
(1) FAS3240AE (Dual Controller Active/Active)
- 24 x 3.0TB SATA Drives (1 x DS4243 shelf)
- 2 x 2054 SAS HBAs (per controller)
- 2x256GB Flash Cache (Performance Acceleration)
- 2 x x1140 10GbE UTA (per controller)
- 72 x 600GB SAS Drives (3 x DS2246 shelves)

Cabinet: Cabinet shown for illustration purpose only.

Cisco UCS BOMs

Cisco UCS
(2) 6248UP Fabric Interconnects
(3) UCS 5108 Chassis
- (1) B200 Server Blades, each with:
  - 1 x X5640 CPU (4-core 2.66GHz 12 MB)
  - 4 GB Memory
  - 2 x 300 GB SAS Drives
  - 1 x M81KR VIC
- (1) B200 Server Blades, each with:
  - 1 x X5640 CPU (4-core 2.66GHz 12 MB)
  - 8 GB Memory
  - 2 x 300 GB SAS Drives
  - 1 x M81KR VIC
- (2) B250 Server Blades, each with:
  - 1 x E5640 CPU (4-core 2.66GHz 12 MB)
  - 192 GB Memory
  - 1 x M81KR VIC
- (4) B250 Server Blades, each with:
  - 2 x E5640 CPU (4-core 2.66GHz 12 MB)
  - 384 GB Memory
  - 1 x M81KR VIC
- (3) B250 Server Blades, each with:
  - 2 x X5680 CPU (6-core 3.33GHz 12MB)
  - 256 GB Memory
  - 1 x M81KR VIC

Server and application inventory

Application Name	Application Vendor	App Version	App Server	App Server Version	Server Name	Server OS	vCPU	RAM (GB)	Disk (GB)	Third Mandate
Agresso	Unit4	5.7.1	IIS	7.5	CPACAGRWEB01 CPACAGRWEB02	Win2008R2 DC	2	8		On-Prem
					CPACAGRAPP01		2	12		
Active Strategy	Microsoft	10.7.0.3	IIS	7.5	CPACASEAPPWEB	Win2008R2 DC	2	4		TBD
Ceridian	Ceridian		IIS		CPACCRDNPROD01 CPACCRDNPROD02	Win7	1	4		On-Prem
Dynamics CRM	Microsoft		IIS	7.5	CPACPRODADFSWS	Win2008R2 DC	1	4		TBD
	Microsoft	2013	IIS	7.5	CPACPRODCRM2013		2	6		
Active Directory	Microsoft		-	-	CPACDC01 CPACDC02	Win2008R2 DC	1	4		On-Prem
Microsoft Exchange	Microsoft	2010	IIS	7.5	CPACMBX01 CPACMBX02	Win2008R2 DC	2	16		Retire

Application Name	Application Vendor	App Version	App Server	App Server Version	Server Name	Server OS	vCPU	RAM (GB)	Disk (GB)	Third Mandate
					CPACCAS01 CPACCAS02		2	12		
File Server	Microsoft		-	-	CPACFS01	Win2008R2 DC				On Prem
MS SQL Server	Microsoft	2008R2	-	-	CPACPRODDB	Win2008R2 DC	2	24		Retire
		2008R2	-	-	CPACPRODSQL01	Win2008R2 DC	2	32		Retire
		2012R2	-	-	CPACPRODMSSQL01	Win2012R2 DC	1	16		On Prem
			-	-	CPACPRODMSSQL02		2	32		On Prem
		2008R2	-	-	CPACPRODMSSQL03	Win2008R2 DC	4	24		On Prem
MySQL	MariaDB	5.5.41	Apache	2.4.6	CPACPRODMYSQLDB01	RHEL 7	1	8		On Prem
Moodle	Moodle	2.9.4+	Apache	2.4.6	CPACPRODMDLWEB01 CPACPRODMDLWEB02	RHEL 7	1	4		Azure
ElasticSearch	Elastic	2.2.1	Apache	2.4.6	CPACPRODSEARCH01	RHEL 7	1	16	50	Azure
Canadian Cancer Trials	Partnership	-	IIS	7.5	CPACPRODWS1 CPACPRODWS2	Win2008R2 DC	1	8		On Prem
Virtual Hospice (Partner)	Venuiti	-								TBD
Endeca	Oracle		IIS	6	CPACPRODEND	Win2003R2	1	8		On Prem
Virtual Hospice (Partner)	Venuiti	-	IIS	7.5	CPACPRODCVH	Win2008R2 DC	1	8		TBD
OncoSim	Beyond2020	-	IIS	7.5	CPACPRODMODWEB	Win2008R2 DC	1	8		On Prem
					CPACPRODMODMDL1		8	32		On Prem
					CPACPRODMODMDL2 CPACPRODMODMDL3		8	32		Azure
EmpowerID	EmpowerID	2014	IIS	8.5	CPACPRODWEB01 CPACPRODWEB02	Win2012R2 DC	4	8		On Prem
					CPACPRODEIDAPP1 CPACPRODEIDAPP2		4	12		
Oracle APEX	Oracle	12c	Weblogic	12c	CPACPRODORA01	RHEL 7				On Prem
Terminal Server	Microsoft		IIS	7.5	CPACTS01	Win2008R2 DC	2	16	100	On Prem

Environment: Peer 1 Toronto II, 151 Front St. (Development, Staging, Disaster Recovery)

Physical Infrastructure: 151 Front (Dev, Stage, Disaster Recovery)

Network / Storage BOM

Cisco Nexus Switching
(1) Nexus 5548UP Chassis each with:
— (1) Layer 3 Daughter Cards
— (1) Nexus 2248TP-E 48 port 1GbE (RJ45) remote linecard
— (2) Nexus 2232PP 32 port 10GbE (SFP+) remote linecard
(2) Nexus C1010 Appliance

Cisco Networking Services
(1) Global Site Selector 4492R Appliance
(2) Application Control Engine 4710 Appliance
(2) Adaptive Security Appliance 5510 with:
— (1) AIP-SSM-20 IPS/IDS Daughter Card

NetApp Storage
(1) FAS3240AE (Dual Controller Active/Active)
— 24 x 3.0TB SATA drives (2 x DS4243 shelf)
— 2 x 2054 SAS HBAs (per controller)
— 2 x 256GB Flash Cache (Performance Acceleration)

Cisco UCS BOMs

Cisco UCS
(2) 6248UP Fabric Interconnects
(3) UCS 5108 Chassis
— (1) C200 Server Blades, each with:
- 1 x X5680 CPU (6-core 3.33GHz 12 MB)
- 4 GB Memory
- 2 x 300 GB SAS Drives
- 1 x M81KR VIC
— (1) C200 Server Blades, each with:
- 1 x X5680 CPU (6-core 3.33GHz 12 MB)
- 8 GB Memory
- 2 x 300 GB SAS Drives
- 1 x M81KR VIC
— (2) C250 Server Blades, each with:
- 1 x E5640 CPU (4-core 2.66GHz 12 MB)
- 384 GB Memory
- 1 x M81KR VIC
— (3) C250 Server Blades, each with:
- 1 x E5640 CPU (4-core 2.66GHz 12 MB)
- 192 GB Memory
- 1 x M81KR VIC
— (3) C250 Server Blades, each with:
- 2 x X5680 CPU (6-core 3.33GHz 12MB)
- 256 GB Memory
- 1 x M81KR VIC

Cabinet: Cabinet shown for illustration purpose only.

Server and application inventory

Application Name	Application Vendor	App Version	App Server	App Server Version	Server Name	Server OS	vCPU	RAM (GB)	Disk (GB)	Third Mandate
Agresso	Unit4	5.7.1	IIS	7.5	CPACDEVAGRWEB01 CPACDEVAGRWEB02	Win2008R2 DC	1	4		On Prem
					CPACDEVAGRAPP01		1	4		
					CPACSTAGAGRWEB01 CPACSTAGAGRWEB02		2	4		
					CPACSTAGAGRAPP01		2	4		
Active Strategy	Microsoft	10.7.0.3	IIS	-	CPACSTGASEAPPWB	Win2008R2 DC	2	4		TBD
Active Directory	Microsoft		IIS	-	CPACDC04	Win2008R2 DC	1	4		On Prem
			IIS	-	CPACDEVDC01 CPACSTAGDC01	Win2012R2 DC	2	4		On Prem
Microsoft Exchange	Microsoft	10	IIS	7.5	CPACMBX03	Win2008R2 DC	2	16		Retire

Application Name	Application Vendor	App Version	App Server	App Server Version	Server Name	Server OS	vCPU	RAM (GB)	Disk (GB)	Third Mandate
				-	CPACCASDR		1	4		
File Server	Microsoft		-	-	CPACFS02	Win2008R2 DC				On Prem
MS SQL Server	Microsoft	2008R2	-	-	CPACPRODSQLDR	Win2008R2 DC	1	4		On Prem
			-	-	CPACSTAGDB		4	32		Retire
			-	-	CPACTESTDB					Retire
			-	-	CPACDEVAGRSQL01		1	6		Retire
		2008R2	-	-	CPACDEVMSSQL01	Win2008R2 DC	4	16		On Prem
		2012R2	-	-	CPACDEVMSSQL02	Win2012R2 DC	2	8		
		2008R2	-	-	CPACSTAGMSSQL01	Win2008R2 DC	1	16		
		2012R2	-	-	CPACSTAGMSSQL02	Win2012R2 DC	2	16		
MySQL	MySQL	5.5.41	Apache	2.4.6	CPACDEVMYSQLDB01 CPACSTAGMYSQLDB01	RHEL 7	1	4		On Prem
Moodle	Moodle	2.9.4+	Apache	2.4.6	CPACDEVMDLWEB01 CPACSTAGMDLWEB01 CPACSTAGMDLWEB02	RHEL 7	1	4		On Prem
ElasticSearch	ElasticSearch	2.2.1	Apache	2.4.6	CPACDEVSEARCH01 CPACSTAGSEARCH01	RHEL 7	1	16	50	On Prem
Canadian Cancer Trials	Partnership		IIS	7.5	CPACTESTWS1 CPACSTAGWS01 CPACSTAGWS02	Win2008R2 DC	1	8		On Prem
Endeca	Endeca Technologies		IIS	6	CPACTESTEND CPACSTAGEND	Win2003	1	8		On Prem
OncoSim	Beyond2020	-	IIS	7.5	CPACSTAGMODWEB	Win2008R2 DC	1	8		On Prem
		-			CPACSTAGMODMDL1		4	32		On Prem
		-			CPACSTAGMODMDL2 CPACSTAGMODMDL3		4	32		Azure
EmpowerID	EmpowerID	2014	IIS	8.5	CPACDEVWEB01	Win2012R2 DC	4	12		On Prem
					CPACDEVEIDAPP1		4	12		On Prem
					CPACSTAGWEB01 CPACSTAGWEB02		4	8		On Prem
					CPACSTAGEIDAPP1 CPACSTAGEIDAPP2		4	12		On Prem
Oracle APEX	Oracle	12c	Weblogic	12c	CPACDEVORA01 CPACSTAGORA01	RHEL 7	1	2		On Prem

Environment: SaaS

Pagely

The Partnership leverages a secure, fully managed WordPress environment by Pagely for hosting WordPress sites.

- Pagely website: https://pagely.com/tech/

Igloo Software

The Partnership leverages an online collaboration tool called Igloo software to support collaboration among internal staff, external stakeholders and partners and its Records management Program. Igloo is made available to the Partnership as a Software-as-as-Service (SaaS) model. A Partnership on premise binary server has been integrated with the Igloo SaaS tool for storage of document objects.

- Igloo Software website: https://www.igloosoftware.com/product

vSphere Capacity Report

	CPU Capacity	Memory Capacity	Storage Capacity	Virtual Machines
Primary DC	226 GHz	2.62 TB	30 TB	78
Secondary DC	172 GHz	2.06 TB	17 TB	129

Hardware Inventory for One University Ave. Office

- Laptops
  - 144 Lenovo laptops
  - 10 Mac laptops
- Docking station
- Docking station key
- Security cable and lock/key
- Monitor
- Wireless keyboard
- Wireless mouse
- Desk Phone (Cisco IP Phone)
- Desktop Printers
- Mobile Phones
  - 61 iPhones
  - 10 Blackberries

Software Inventory at One University Ave. Office

Software	Installed on PC	Installed on mobile	Accessed through Web	System Admin	End User
Active Strategy			X		X
Adobe Acrobat Professional	X				X
Adobe Acrobat Reader	X	X			X
Adobe Creative Cloud	X				X
Adobe Design Premium	X				X
Adobe Flash	X				X
Adobe Indesign	X				X
Adobe Shockwave	X				X
Agresso	X		X		X
Agresso Reports		X			X
Blue Jeans		X	X		X
Cisco Jabber	X	X			X
Cisco VPN Connect and AnyConnect	X	X			X
Eeminders	X				X
EndNote	X				X
Evernote	X	X			X
GoToMeeting		X			X
GoToWebinar		X			X
Google Authenticator		X		X	
Google Chrome	X	X			X
Igloo			X		X
Igloo Desktop	X				X
Internet Explorer	X				X
IP Communicator	X				X
Irfanview					
Java	X				
Kaseya	X			X	
Logitech Unifying Software	X				
McAfee Endpoint Protection	X				
Meraki Systems Manager		X		X	
Microsoft Dynamics CRM			X		X
Microsoft Dynamics CRM Outlook Plug-in	X				X

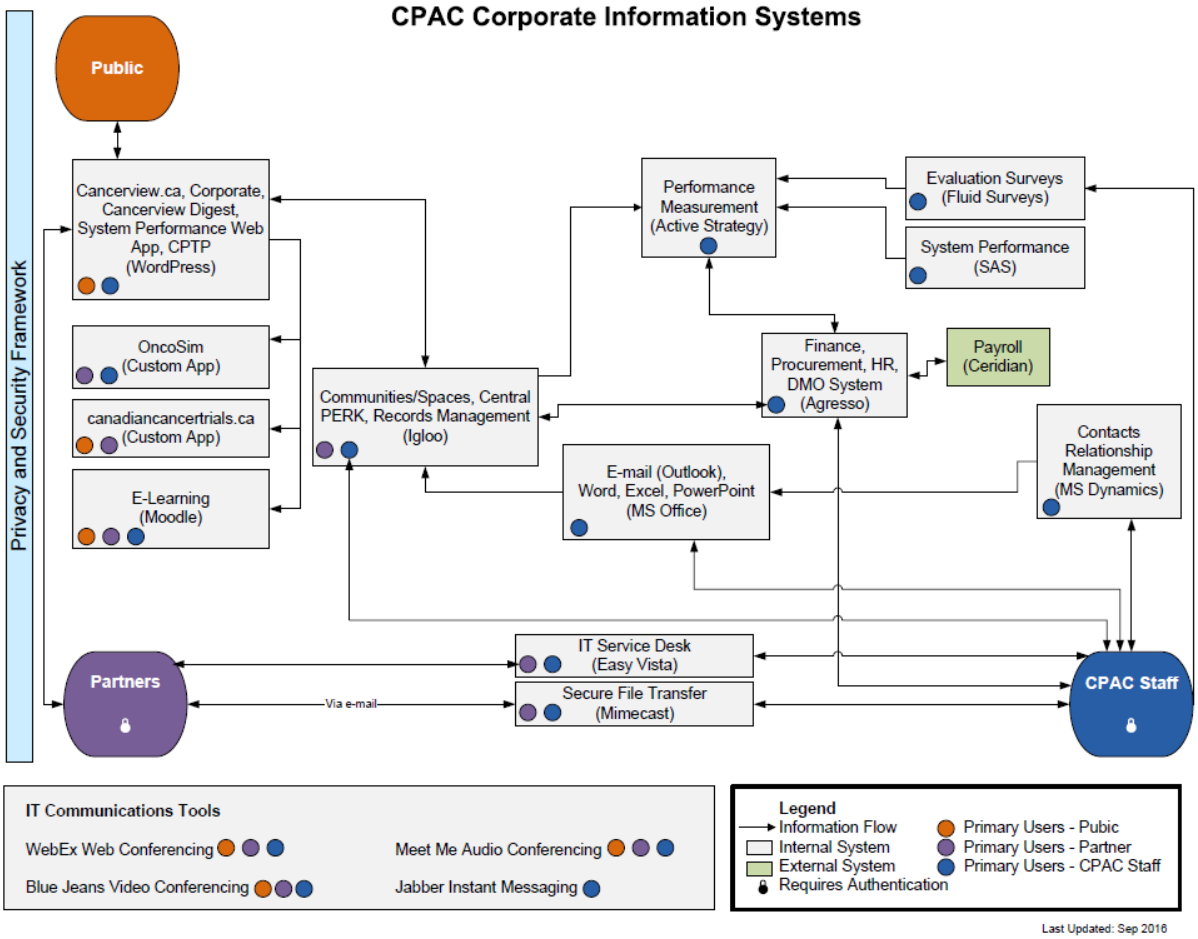
Microsoft Office 2013	X				X
Microsoft Outlook 2013	X				X
Microsoft Project 2013	X				X
Microsoft SQL Server Management Studio	X				
Microsoft Visio 2013	X				X
Microsoft Visual Studio 2008	X				X
Mimecast		X	X		X
Mimecast Outlook Plug-in	X				X
Moodle			X		X
Mozilla Firefox	X				X
My Data Manager		X			X
Oracle SQL Developer	X				
OrgPlus			X		X
PDF995	X				X
PowerMapper	X				
Putty	X				
Reference Manager					
Safari	X				X
SAS	X				X
SnagIt	X				X
SortSite	X				
SVN	X				
VMware Player	X				
WebEx		X	X		X
WebEx Productivity Tools	X				X
Windows 7	X				X
WinSCP	X				

Standard Operating Procedures (SOPs)

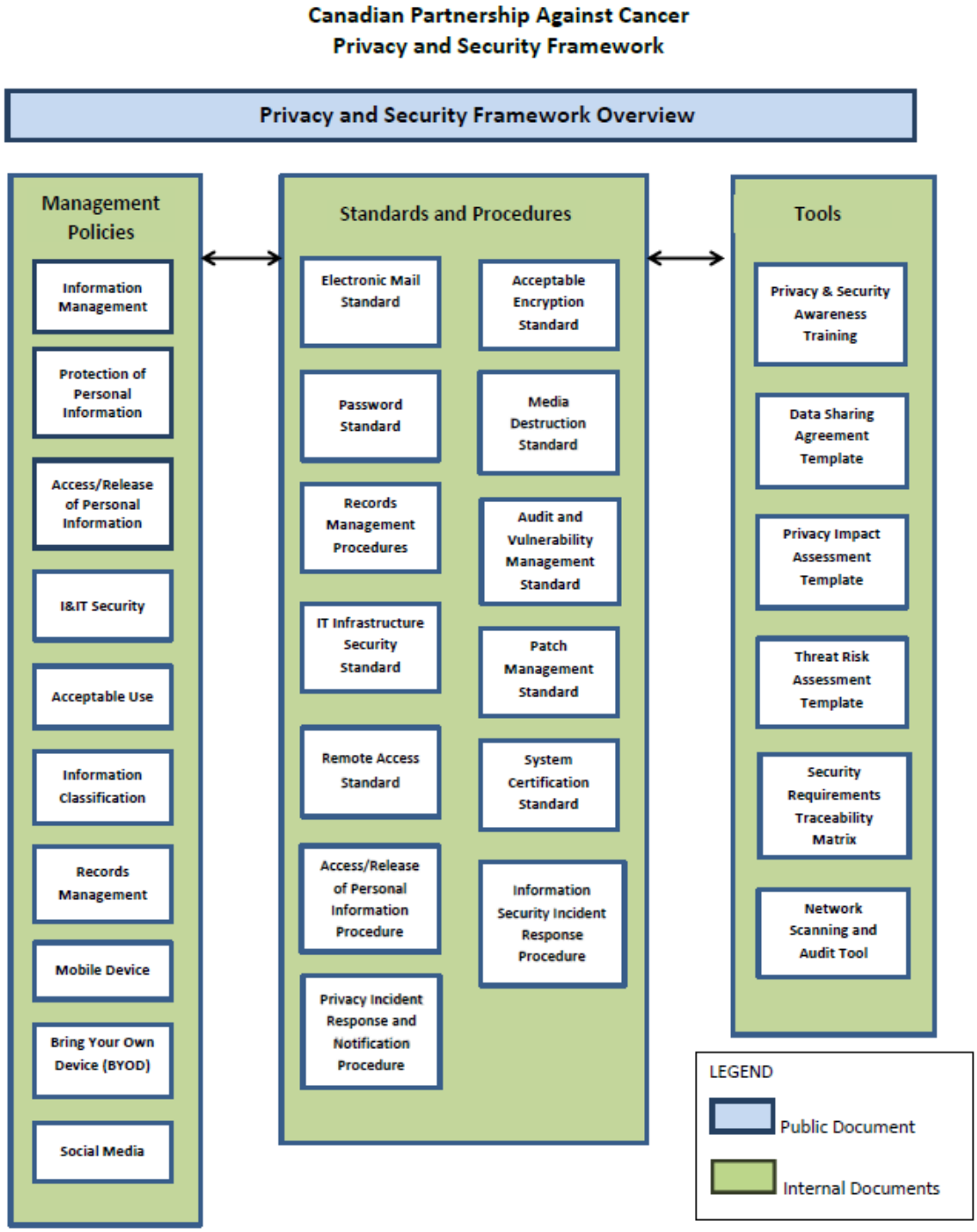
- Employee Onboarding
- Employee Role Change
- Employee Off boarding
- Infrastructure/System Patching and Maintenance
- Central PERK Intranet
- Records Management
- Remote Access

- Security Escalations
- Change Requests
- Application Management
- Network Management
- Troubleshooting
- Accounts, Access, and Permissions
- Notifications

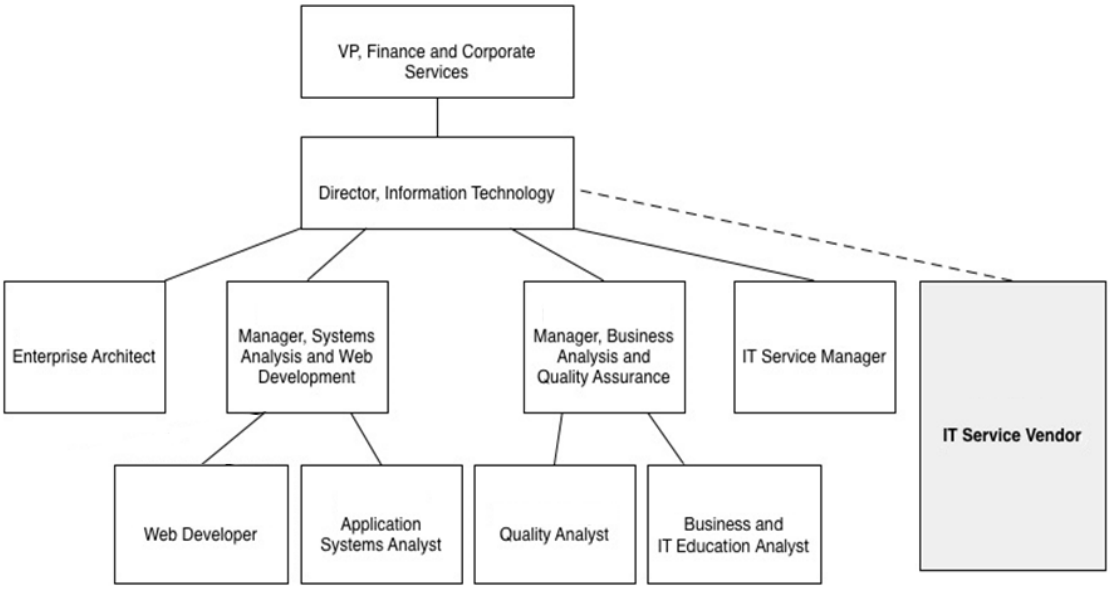
Corporate Information Systems Diagram



Privacy and Security Framework



Information Technology Team Organization



Future State Information

IT Infrastructure; Future State

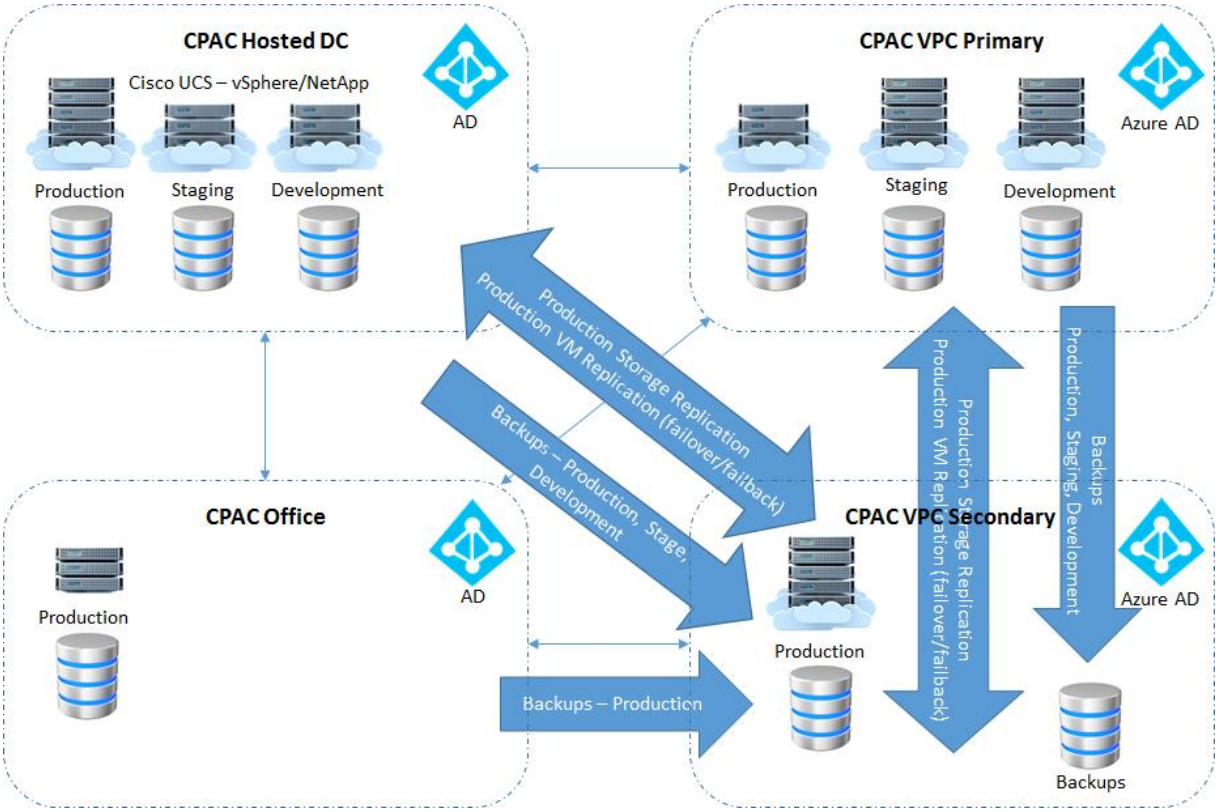
The Partnership is currently evaluating cloud service opportunities and planning to transition additional workloads to SaaS/PaaS/IaaS vendors to reduce overhead/complexity and focus more Partnership resources on core business initiatives while providing better value and flexibility for the Partnership. Current internal initiatives such as OncoSim, a microsimulation tool, are also driving the need for an on-demand computing resource model to support dynamic scaling.

The Partnership is planning to displace the functionality provided by our secondary data center with the Microsoft Azure Cloud for backups, disaster recovery and extended compute capacity during the early part of the contract period. This should reduce the capacity and complexity required at our primary data centre; and reduce the Partnership's operating and capital expenditures required to manage/maintain a secondary data centre.

The Partnership will continue to evaluate new cloud service opportunities throughout the course of the contract period to identify additional areas of benefit to the Partnership. The success and experience garnered from transitioning our secondary data center to the Microsoft Azure Cloud will have a significant impact on future IT planning, transition and adoption.

The successful Proponent will be a significant partner involved in the transformation from an on premise/co-located infrastructure to a cloud based infrastructure.

Future Hybrid Cloud Configuration



5-year Growth Projections for Key Metrics

Metric	Current Level	Projected Level over Contract Period
# of Total Staff (including permanent, temporary, contract staff, paid advisors and students)	156	156
# of Work-From-Home/offsite Partcipants (including 17 individuals that are expert leads and senior scientific leads)	45	45

# of IT Staff	9	10
# of On-site Service Desk	1	1
One University Office Space	2100 square feet	2500 square feet**
File Storage	35 TB used / 50 TB avail	200 TB
Network Availability	24x7	24x7
Systems Availability	99.9%	99.9%
Recovery Time Objectives	24 -48 hours	24 - 48 hours
On-site Support Hours	Monday to Friday (8am – 6pm, Toronto Time), 7x24 for critical and urgent failures	Monday to Friday (8am – 6pm Toronto Time), 7x24 for critical and urgent failures
On Call after-hours Support Hours	Monday to Friday (6am – 8am and 6pm to 11pm, Toronto Time)	Monday to Friday (6pm to 9pm Toronto Time)
Average Number of Monthly Service Desk Incidents	160 (90 calls)	Goal is to reduce the average number of Incidents over the contract period

**** The Partnership is currently conducting an office lease review. There is the possibility the Partnership will move office locations sometime after April 1, 2017.

EXHIBIT B – Project Work Requirements

Introduction

This Exhibit pertains to the project work portion of the RFP that will be carried out during the transition period of January 2, 2017 to March 31, 2017 and periodically between April 2017 and March 2022 as required and directed by the Partnership.

The goal of the work during the transition period will be to achieve a state of support readiness by transitioning all support services and infrastructure under the Partnership's current support contract by March 31, 2017. Project activities should include; planning, analysis, design, installation, configuration and implementation of infrastructure, information systems and supporting process and procedures.

All infrastructure hardware required for the transition phase will be provided at cost effective rates, ensuring alignment with the Partnership's procurement practices. The Proponent should evaluate and leverage the Partnership's existing assets and resources where possible.

For on-going project work after April 1, 2017, the Partnership will work with the Proponent to plan and scope project initiatives on an as required basis resulting in the Proponent developing a Statement of Work and corresponding budget based on the rate sheets agreed to under this contract. For the purposes of on-going project work after April 1, 2017, a project will be defined as follows.

Definition of a Project
A project is defined as research, analysis, planning, design, installation, configuration or implementation that creates a unique output for the Partnership. For the purposes of this agreement, this is anticipated to be work involving more than one (1) person and more than forty (40) hours of effort where the project plan, information system or business process does not already exist and where the work has not been performed before as part of the IT Support Service (e.g. Annual software upgrades have a project plan and have been performed before, so although they are >40 hours and more than one person, it would not be a negotiated project requiring a time and materials assessment).

Definition of Success

1. A future state infrastructure that simplifies system administration, reduces the Partnership's overall risk profile and improves operational efficiencies.
2. Ability to create standard operating procedures that are mature and repeatable.
3. Create a clear separation in application architecture and data between the Partnership and its cloud service provider(s).
4. Adoption of industry standards and best practices when utilizing methodologies, theories and designs.

Requirements for Transition Period (January 2017 – March 2017)

B1 Finalize Design of Hybrid Environment

Confirm bill of materials for servers, storage and backup and any other network equipment required for on premise datacenter build which will consolidate the number of the Partnership's data centers from two to one. Identify any additional Azure cloud services needed to support the new hybrid environment.

B2 Build Hardware

Procure, build, configure and test hardware environment. Migrate, install and configure any existing network hardware (e.g. routers, load balancer(s), switches) from current state environment that can be leveraged in the new hybrid environment.

B3 Server Operating Systems

Installation and configuration of all necessary server operating systems. Servers which are exposed to the public internet should be put in the DMZ network behind firewalls with IPS protection. Corporate IT systems should be virtualized and hosted in one network protected by its dedicated redundant firewalls.

B4 High Availability

Production and staging environments should be installed and configured for high availability. The CPU/memory resourcing will be scaled back from the production environment for staging. The test environment should have similar configuration without high availability. UPS installation and configuration will be included.

B5 Corporate Application Stack

Install, configure and migrate VMs and data to the corporate stack of products in the production data center with failover capability to the Partnership's Microsoft Azure cloud site.

The corporate software designated for the on premise data center is outlined in **Exhibit A**.

B6 Unified Communications

Integrate existing Cisco UC platform or new hosted VOIP telephony SaaS solution with Office 365. This would enable the corporate end user environment to be able to listen to their voice mail directly from their Office 365 inbox on a variety of devices including mobile phones and tablets.

B7 Microsoft AD Integration

In the new hybrid environment, configure and integrate Microsoft Azure Active Directory with the Partnership's on premise Active Directory environment.

B8 Dedicated bandwidth

Assess and revise the current dedicated bandwidth between the Partnership and the production data center as required to maintain an acceptable quality of service level. Pipe provisioning between the on premise data center, the Microsoft Azure Cloud site and the One University Avenue office may be required.

B9 Firewall

Installation and configuration of all necessary firewalls, including firewall rules configuration. Ensure firewall hardware and configuration software sparing to ensure rapid replacement in the case of failure. Intrusion detection and protection systems will be installed and configured for client security processes and controls.

B10 Load Balancing

Install and configure all necessary load balancing hardware. Optimize internet performance and improve website response time and reliability. Onsite hardware sparing to ensure rapid replacement in the case of hardware failure will be included. The current data center environments have load balancing capabilities to assist with standardizing the user experience and assisting with availability management efforts.

B11 Data Migration and Systems Configuration

Migrate all software system configurations and data to the new hybrid environment.

B12 Baseline measurements

Load test configuration and take baseline measurements for all internal system points of failure or bottlenecks and put the capability in place to access all migrated systems from an external internet connection for independent performance verification. With the baseline established, scripts and monitoring software should be put into place to regularly and automatically perform a series of comparative performance tests in order to identify if there are any variances at the point of running the test as compared to baseline.

B13 Monitoring Tools

Installation and configuration of network, server and application monitoring should be installed and configured of all environments. Establish performance benchmarks prior to the April 1, 2017 support service go-live.

B14 Performance

A full loopback loading of any application will take four seconds or less. Align the application architecture with the infrastructure architecture for the prioritization and delivery of certain types of traffic i.e. priority/class of service for Voice over IP and the volume of traffic in order to improve the speed and responsiveness of critical applications.

B15 Encryption

Ensure that all unified communications are encrypted, prioritized and controlled by a VPN.

B16 Application Auditing

Implement application auditing for all systems and enable the reporting capability to ensure the systems have a key security component in place, allowing for comprehensive analysis of system changes made (who did what when). Cross system authentication (ideally single sign on for all solutions) or consistency in logins.

B17 Disaster Recovery

Update the Partnership's existing Disaster Recovery Plan by analyzing the various options to meet the Partnership's Recovery Time Objectives as outlined in **Exhibit E, Section E14**. Implement the successful strategy that aligns with the new hybrid environment and ensure the plan can be operationally tested on an annual basis.

B18 Service Desk Orientation

A personalized one-on-one session for each Partnership employee at their workstation will be required in order to orient each employee on the new/revised support personnel and processes prior to the April 1, 2017 support service go-live.

B19 De-commission old equipment

Once the new hybrid environment is operational, dispose of any on premise infrastructure that cannot be leveraged in the new hybrid environment while following the Partnership's requirements for environmentally friendly disposal and secure data wipe (hard disks only).

EXHIBIT C – Service Desk Requirements

Introduction

The Partnership requires a single point of contact service desk to manage Tier 1, 2 and 3 services as per the service catalogues outlined in **Exhibit A**. The successful proponent will take full ownership of each Incident or Service Request created at the service desk until it is resolved and satisfactorily closed regardless of which party is handling the Incident or Service Request.

The successful Proponent's service desk is built and based on ITIL best practices tailored to meet the specific needs of the Partnership and managed to the Service Level Objective requirements outlined in **Exhibit F**.

Definition of Success

1. Having highly qualified service desk technical resources at all times during the contract period.
2. A commitment to continuous quality improvement and following industry best practices.
3. Proactively ensure the environment is operating well by recommending timely fixes, upgrades, changes, training and purchases to the Partnership's IT Service Manager.
4. Proactive communication from the service desk to the end users in the escalation of Incidents, known problems, quick tips, customer complaint follow up and educational sessions as directed by the Partnership.
5. Provide easy and simple user access to information using an up-to-date, detailed and accurate Knowledge Base. Population of known errors and their workarounds in the Knowledge Base.
6. Creation and implementation of training procedures and ITIL best practices/processes to ensure adherence to best practices in order to maintain a high level of customer satisfaction.

Requirements

C1 Single Point of Contact

There will be one point of contact for all service requests including those Incidents that require escalation to external third party organizations. It is the expectation that the successful proponent will manage the existing service desk phone number, 1-866-699-6099, for all support requests.

C2 Location

The Proponent's service desk operation will reside in Canada.

The service desk for on-site support services is currently located at One University Avenue. Onsite resources should be within one (1) hour travel distance to One University Avenue with same day dispatch capabilities.

C3 Availability

The service desk will provide onsite support services with one full time equivalent, skilled resource, Monday through Friday from the hours of 8 am to 6 pm local Toronto time excluding statutory holidays. Onsite support services would be augmented by additional resources and/or remote support staff for capacity and escalation purposes.

The service desk will provide an after-hours call support service from the hours of 6pm to 9 pm local Toronto time Monday to Friday (excluding statutory holidays). The after-hours call management service will make a separate queue available specifically for the Partnership and be seamlessly integrated with the on-site service desk tool described in **Section C16**.

C4 Methodology

The service desk will provide services via phone, e-mail, in person and remotely via web. A vast majority of Incidents will be solved from the use of a helpful, accurate, organized and up to date knowledge base, populated by the service desk based on the history of Incidents and their associated workarounds and resolutions.

It is a requirement that all Incidents that fall inside and outside of the service level objectives be escalated, tracked and reported on including those escalated to external third parties.

C5 French Translation

French translational services will be available if required for service calls from French speaking users. The Service Level Objective requirements outlined in **Exhibit E, Section E14** will apply to all Incidents regardless of the user speaking English or French.

C6 Education & Training

The Proponent will maintain an on-boarding training plan for their staff, keep training records of their staff and ensure all new staff are trained in the functional aspects of the environment they are required to support during the contract period. Training curriculum may be reviewed by the Partnership to ensure learning requirements are met.

The service desk will arrange professional training sessions for Partnership staff as required. The sessions are to be instructor led by a training instructor from a reputable training institution. The training sessions will be organized with the continuous service improvement initiative in mind to decrease the number of Incidents opened at the service desk.

Training curriculum and session content will be curated by the Partnership's Training and Education personnel. Training content may be functional use-cases, hands-on walkthroughs, or technical overviews based on audience.

C7 Customer Satisfaction

The service desk should be a proactive service operation with a focus on quality assurance and continuous improvement. The service desk will send a "customer satisfaction survey (Incident resolution)" to all end users following Incident closure. The service desk should allow for content and format changes to the survey throughout the term of the contract. The "customer satisfaction (Incident resolution)" Key Performance Indicators (KPIs) will be included in the monthly management reporting provided by the service desk analysis and reporting function described in **Section C9**.

The "customer satisfaction survey (Incident resolution)" should be sent as an automated email with the ticket number and description pre-populated so that users can remember which Incident they are being asked to report on one step prior to Incident closure. The end user will confirm the Incident is solved and complete prior to the Incident being closed; re-opened Incident tickets will be measured as a KPI.

The service desk will also send a "customer satisfaction survey (service desk)" to all end users to gather strengths and weaknesses feedback regarding current service desk performance. Responses will be confidential and anonymous. The service desk should allow for content and format changes to the survey throughout the term of the contract. The "customer satisfaction (service desk)" KPIs will be included in the monthly management reporting provided by the service desk analysis and reporting function described in section C9.

Service Desk Key Performance Indicators: Customer Satisfaction Survey (for all surveys)
The satisfaction rating will come from the addition of the "Very Satisfied" and the "Satisfied" responses as a percentage of the total surveys received for the following areas:

1. Promptness
2. Technical Competence
3. Customer Service
4. Communication
5. Overall Satisfaction

An open text question should also be available for the user to type in specific feedback.

C8 Documentation

The service desk will create and present documentation relating to all services provided on an ongoing basis. All documentation should be accurate, up to date, and readily available upon request. The service desk will create knowledge base articles for reference by all levels of service desk personnel as well as the end user community. These articles will be based on resolutions that have been found to common Incidents as well as problems (unknown and known errors). All documentation and knowledge base articles should be stored in the service desk's tool and usage metrics should be tracked and reported upon.

C9 Analysis & Reporting

The service desk will measure quality and provide continuous improvement initiatives to continually refine and improve the Partnership's IT business practices. It is the responsibility of the service desk

to provide feedback for the monthly management report in the form of recommended changes to; policies, standard operating procedures, applications and infrastructure.

The following will be incorporated into the monthly management reporting process.

1. Analyze the volume of Incidents created at the service desk and in turn recommend training needs in the area creating the highest volume and/or frequency of Incidents.
2. User satisfaction survey results.
3. Allow for flexibility as reporting requirements may change from time to time.
4. Allow for reporting by tier, role, Incident status and priority.
5. Produce an exception based report by role indicating Incidents that have exceeded Service Level Objectives targets for resolution or have passed 80% of the time allotted for resolution.
6. Produce a summary report indicating the number of cases opened in the previous reporting period sorted by role, Incident status and then by priority in ascending order (or example each role will list all open cases of the highest priority first).
7. Produce a detailed report indicating Incidents with a status of open and sorted by priority in ascending order.
8. Report on KPIs with monthly, quarterly, and rolling trends indicating:
    a) First Call Resolution Rates
    b) First Contact Resolution Rates i.e. no escalation required
    c) Performance of service elements against their respective service level objective targets
    d) Number of Incidents and percentage increase or decrease in the total number of Incidents resolved for a tier and/or a role
    e) Average resolution time and percentage increase or decrease in the average resolution time of Incidents for a tier and/or role
    f) Number of abandoned calls and the percentage increase or decrease in the number of abandoned calls
    g) Balanced scorecard across key selected metrics as agreed to with the Partnership
    h) KPIs from knowledge center support
9. Adjust current metric and KPI gathering methodology or create net new as necessary to meet analysis and reporting needs

The following reports are expected to be provided as part of the Services. Issues may arise and reports will be required to be made available on an as needed basis.

Report	Frequency
Backup Verification Log	Daily
Service Improvement Plan	As Required Following a service disruption or discrepancy
Incident Report	As Required Following a security incident or unplanned network outage.
Service Desk Report	Weekly An analysis of open service desk tickets
Software License Compliance Report	Quarterly
Management Report	Monthly Includes KPI performance results and continuous improvement recommendations
Inventory Report	Quarterly A summary of all hardware and software assets
Trending Report	Quarterly Includes Incident, software and infrastructure trends and analysis.
Disaster Recovery Test Report	Annually Results and recommendations from the annual DR testing
Quality Review Report	Annually Includes the analysis and recommendations from an annual review of services.

C10 Data Backup Retention and Availability

All service desk data including reports and surveys will be electronically archived in a database format for future reference for the duration of the contract period. The data should be readily available and transferable in a standardized format (ie.csv) and remains the intellectual property of the Partnership. All data from the entire contract period needs to be transferred to the Partnership upon contract termination.

The service desk is responsible for checking the activity logs from the backup solution on a daily basis and emailing proof of success. If the backup was unsuccessful, an error report needs to be sent with the work-around date, time and procedure. Results from quarterly backup and restore testing should be also e-mailed to the Partnership's IT Service Manager. All backups and restorations should be tested. An Incident should be created each quarter and assigned to the resource responsible for the testing.

C11 Incident Classification

The service desk will assess the Incident details and select the appropriate classification after performing first level troubleshooting and diagnosis. The service desk will conduct an initial

assessment of urgency and impact and assign the Incident an appropriate priority level. Examples of known Incidents are prioritized in the Priority Levels table below. The service desk will use the Urgency and Impact Categorization Tables and Priority Matrix below to determine the priority that will be assigned to Incidents.

C12 Incident Categorization

The service desk will categorize each Incident accurately. Incident categorization will take into account the level of user impact. Immediate and upcoming known issues that would degrade performance or impede user's ability to perform work should have proactive notifications to users (classified as "User Impacting" issues) and have the appropriate communications and follow-ups for assurance.

Priority Levels

Priority	Conditions	Response Time and Commence Time	Resolve Time
1 Critical	Total or substantial loss of availability or functionality to all sites and end users A major service disruption which has an impact on users including but not limited to; ✓ Digital Properties ✓ Collaboration (includes Intranet) ✓ Identity Management ✓ Records Management ✓ Agresso A major service disruption which has an impact on the web conferencing service including; ✓ Teleconference ✓ Webcast A major service disruption which has an impact on the corporate users including but not limited to; ✓ File, Print, Email and Calendar	The maximum response time to assign an Incident # is 15 minutes Incident escalation, dispatch and technical resource allocated within 15 minutes of Incident creation during the hours 8 am – 6 pm	4 hours (Same Business Day with continuous effort if not resolved within target Resolve Time) From the time Incident was created will equal 4 hours

	✓ Phone, Network, VPN		
2 High	Loss of significant availability or functionality to multiple sites and/or end users A severe impact on website and corporate users including but not limited to; ✓ eLearning ✓ OncoSim (formerly called Cancer Risk Management) ✓ Finance ✓ Payroll ✓ Backup unsuccessful ✓ File, Print, Email and Calendar ✓ Service Desk ✓ Password resets	The maximum response time to assign an Incident # is 30 minutes Incident escalation, dispatch and technical resource allocated within 30 minutes during the hours 8 am –6 pm	4 hours (Same Business Day with continuous effort if not resolved within target Resolve Time) From the time Incident was created will equal 5 hours
3 Medium	Any loss of application availability or functionality to one or more sites and/or one or more end users Minimal impact on service and individual end users including but not limited to; ✓ Permissions, Access ✓ Patch installations	The maximum response time to assign an Incident # is 30 minutes Incident escalation, dispatch and technical resource allocated within 2 hours during the hours 8 am – 6pm	8 hours (Next business day) (From the time Incident was created will equal 10 hours)
4 Low	No sites are affected Minor or no impact on service including but not limited to;	The maximum response time to assign an Incident # is 30 minutes	5 business days

	✓ Request for information, request for training	Technical resource allocated within next 1 business day during the hours 8 am – 6 pm	(From the time Incident was created will equal 4 days)
5 Planning	Requests for improvements or additional application functionality including but not limited to; ✓ Corporate moves and change ✓ Software Upgrades	The maximum response time to assign an Incident # is 30 minutes	10 days

Service Desk Urgency Categorization

Category	Description
High (H)	• Incident has a high impact and requires immediate attention and resolution.
Medium (M)	• Incident has defined impact and requires quick response and resolution.
Low (L)	• Incident has a low impact and can wait until the standard update or change is available or upon mutually agreed resolution target.

Service Desk Impact Categorization

Category	Description
High (H)	• A critical service is unavailable to the Partnership user community, or the Partnership cannot conduct critical business operations.
Medium (M)	• A critical service is degraded or a non-critical service is unavailable to the Partnership user community, or may be affecting a group of individuals or teams.
Low (L)	• A non-critical service is degraded or affecting an individual and a work-around is available.

Priority Matrix – Service Desk will use the matrix below to determine the priority that will be assigned based on the Impact and Urgency of the Incident.

		Urgency		
		High	**Medium**	**Low**
Impact	**High**	Priority 1 - Critical	Priority 2	Priority 3
	Medium	Priority 2	Priority 3	Priority 4
	Low	Priority 3	Priority 4	Priority 5

C13 Communication

The minimum requirements for service desk communication are outlined in the following chart:

Sense of Urgency	Frequency	Methodology
Critical Priority Level 1 Incidents The Proponent will have a communication system in place to inform callers of the impacts, durations and expectations of a particular planned or unplanned event and a major Incident response team process	On Demand	Phone and E-mail Submit urgent mission critical priorities via phone to the assigned party and place a second call to their escalation contact to inform them of the situation and the status. The desire is that all callers will remain in the queue unless they choose to abandon the call.
High Priority Level 2 Incidents	On Demand	Phone and E-mail Submit urgent mission critical priorities via phone to the assigned party and place a second call to the escalation contact to inform them of the situation and the status.
Medium Priority Level 3 Incidents	Weekly	Email via the Open Incident Report - submit a daily Incident report of all Incidents that have fallen outside of SLA via e-mail. The daily Incident report needs to highlight the party responsible for the Incident. The report also needs to highlight green for tickets that have been resolved that previously were in the escalation report for the week in question, yellow for those that have just reached SLA and red for those that are over SLA.

		Alternatively, provide the capability of the Partnership IT Service Manager to run the report and obtain statistics.
Low All Incidents	Daily	E-mail a satisfaction survey URL to each Incident holder populating the Incident number and description for the end user to respond with their satisfaction rating. Ensure that a blank field is available for comments and feedback. E-mailing this link prior to incident closure provides the end user with the opportunity to disagree with the closing of the ticket.
Planned	Monthly	E-mail and In person via the monthly Management Report. This report will be received within six (6) business days of the preceding month. Meet in person with the Partnership to review incidents for escalation, service level agreement adherence and service level improvement plans. Review Trending

Service Desk Manager (Proponet), IT Service Manager and Director of IT to meet face to face on a monthly basis to:

1. Review the monthly management report, and any service improvement plan reports. This portion of the meeting will focus on the current state.

2. Review the contract, service level agreement and balanced scorecard. A discussion around action plans for remedying Incidents that have fallen outside of SLA will result in the creation of new Service Improvement Plans.

3. Continuous Improvement opportunities should be presented by the Proponent with feedback from all Tier levels of support resources, subcontractors and management teams.

C14 Required Skills and Experience

The Proponent should be able to demonstrate sound hiring and end-of-employment practices, including:

1. Details of hiring policy, and background checks that are conducted before a staffing vacancy is filled.
2. Details of policy and practices followed upon termination of staff employment.
3. Demonstration of ability to backfill for resources who may inadvertently not be able to report to work.
4. Demonstration of ability to mobilize necessary and adequate staff, both administrative and technical, in cases of emergency including accidental hardware failures, security breach and requirement to support audit and forensic investigative initiatives initiated by the Partnership.

The skills required for personnel supporting this contract are as follows and will be taken into consideration in the scoring of Stage 2C:

Service	Certification, Education and Experience Required
Service Desk	• A minimum of four (4) MCSAs Windows 10 • A minimum of two (2) ITIL v3 Foundations certified personnel • Service desk resources should have (3) years minimum experience supporting MS Office environment
Managed Hosting	• A minimum of one (1) CISSP (Certified Information Systems Security Professional) • A minimum of one (1) MCSE Server Infrastructure • A minimum of one (1) CCNA (Cisco Certified Network Associate Routing and Switching) • Should have support arrangements and ongoing relationship with Cisco TAC • A minimum of one (1) Virtualization expert (VCP) in VMware technology with a path to achieve VCP5 within one (1) year. • A minimum of one (1) Backup & Storage expert for the proposed Backup & Storage solution • A minimum of one (1) Linux system administrator familiar with Red Hat (RHCSA preferred) • A minimum of one (1) MCSD Azure Solutions Architect
Application Management	• A minimum of five years' experience in enterprise vendor and project management, preferably in a Managed Services Provider context.

The Partnership should be notified in writing with an updated profile when proposed resource changes occur such as backup personnel becoming primary personnel and new backup personnel arriving. The Partnership should be given the opportunity to meet key personnel dedicated to the account three weeks in advance prior to their recruitment and arrival. New key personnel should present proof they are trained in baseline familiarity of the Partnership's operational processes before the Partnership accepts the changes.

C15 Knowledge Base

A knowledge base facilitating a self-help environment is essential. This will be considered successful when the first call resolution rate will trend downward as customers start answering their own questions for routine Incidents, leaving the more challenging Incidents for the service desk. The service desk will need to be able to integrate self-service measures into the measurement, reporting and trending process.

Connectivity and transferability between the service desk tool and the Partnership's applications (wikis, WordPress, Central Perk) is required. Ideally, the service desk tool's knowledge base capabilities will be used as the integrated single source of truth with dynamic links for the Partnership's knowledge articles that cannot be integrated.

Knowledge articles will need to cater to both technical and non-technical users. Especially important for self-service solutions, simple-to-follow steps should be prominently displayed with following underlying technical details.

Service desk training is a large component to ensuring the knowledge center support solution is successful. Continual reference to and population of the knowledge base are essential to it becoming an effective tool for the service desk and for the end user environment. The following KPIs should be measured. Changes to KPI requirements may occur during the lifetime of the contract as determined by operational requirements.

Key Performance Indicator

a) Total number of solutions available

b) Number of Incidents resolved using the knowledge base

c) Percent of Incidents resolved using the knowledge base

d) Number of times customers access the knowledge base

e) Number of escalations to the support center via the web

f) Number of frequently asked questions

C16 Service Desk Tool

A new enterprise level service desk tool will be required because the current tool, EasyVista, no longer meets the Partnership's requirements. The IT Service Support Management (ITSSM) tool will adhere to ITIL standards, be a SaaS based solution and should be included on Gartner's Magic Quadrant for ITSSM 2016; the specific tool will be determined based on the Proponent's experience and recommendation. The Proponet should be experts in the configuration, deployment, and maintenance of the service desk tool.

Pricing

The Partnership will leverage the service provider's discounted pricing for the SaaS service desk tool, if available via resale. The Partnership will retain all rights to the tool's custom configuration, documentation, and workflows.

Portal
The tool should have a configurable web-based portal that would allow IT to prominently display notifications and allow users to: self-service requests, check current status for Incidents and requests, updated Incidents, report issues, and self-serve FAQ and knowledge articles. The Proponent will design and maintain the portal with input and guidance from the Partnership.

Service Requests
All service requests will incorporate e-signatures in a fully functional workflow. Automated self-service requests will be enabled with configuration service requests categories such as "Standard Requests" to enable automated approval and deployment workflows; specifics of "Standard Requests" will be determined during tool planning phase.

Known Error Database
A known error database (KEDB) should be integrated with the tool. The KEDB will be used to allow the service desk to direct users to known errors and their work-arounds. The KEDB should be treated as Knowledge Centered Support and continuously updated.

Functionality Requirements
Ticketing

Requirement Description	Required (R) or Optional (O)?
Provide the ability to each Client Service Desk to view ticket status via the Web.	R
Provide an integrated "portal experience" for users to interface with IT	R
Online lists of pending requests and problems	R
Ability to log, diagnose, and resolve tickets	R
The ability to specify components affected by a reported Incident	R
Ability to prioritize, assign, and track problems and Service Requests	R
The ability to detect open problems for which the resolution time has been exceeded	R
Statistical analysis of repetitive Incidents and trends	R
Capability to generate reports and identify repetitive Incidents and trends	R
System monitoring to proactively detect underlying problems	R
A facility to establish relationships between detected problems and related Incidents	R
Generate detailed and summary reports on Incident management for comparison with target SLAs	R

Detailed and summary reports on activities by problem type, system type etc.	R
Time of service outages detailed for SLA reporting	R

Incident Management

Requirement Description	Required (R) or Optional (O)?
Incidents logged, relevant information recorded	R
Information about the user being provided automatically as users call in	R
Repeat calls are tracked and reported	R
Proactive Incidents resolution: Users notified of known Incidents before they report the Incident	O
Incidents associated with those previously reported/determined by support personnel	R
Tracks Incidents against SLAs/Maintenance contracts and corrects accordingly	R
Incidents analyzed	O
Incident resolution prioritized	R
Resources being assigned to resolve incident (one or more resources may be involved)	R
Incident Databases and archives being utilized to determine potential solutions	R
Incident related and linked to problems	R
Unsolved Incidents escalated to problems	R
Incident resolution progress tracked, updated in log	R
Users notified of Incident status, resolution or non-resolution	R
Solution for the Incident stored in the knowledge database	R
Information distributed to users for Incidents on the most common problems and their solution, and of known work-arounds	R
Reports automatically generated for Incidents, their solution and performance, and sent to appropriate parties	R
Future Consideration: Linkage to Organization Change Control Tools/Change Management	O

Problem Management

Requirement Description	Required (R) or Optional (O)?
Process provides a “rapid resolution” approach for major outages/service impacts	R
Toolsets in place to log, track, manage, and report all problems	R
Each level of the problem escalation path can be tracked for progress, performance, outstanding problems, compared to SLAs, etc.	R
Users are provided self-support mechanisms/tools (FAQs, Technical Briefs, on-line help, etc.)	R
Problem resolution prioritized, resources assigned accordingly	R
Problems categorized, updated in log, archived, linked etc.	R
Future Consideration: Change request issued	O
Problems linked to service request/change request	R
Problem resolution tested after order has been fulfilled	O
Reports automatically generated for Incidents, their solutions and performance are sent to appropriate teams	R

Configuration Management

Requirement Description	Required(R) or Optional (O)?
Overview of service assets to aid other processes, such as Change and Incident management	R
Automated asset discovery	O

C17 Annual Quality Review

The successful Proponent will be expected to commission an annual quality review of their implemented IT Solution with the first review to occur in early 2018 and each year thereafter within the contract period.

EXHIBIT D - Application Management Requirements

Introduction

The main goal of this support function is to create and maintain a successful, timely and impact free application environment for the Partnership.

The Partnership is seeking technically deep expertise in managing and maintaining its suite of applications as detailed in **Exhibit A**. The Partnership requires assurances from the Proponent that the adequate levels of required technical skilled resources as outlined in **Exhibit C, Section C14** will be available consistently throughout the contract period.

Definition of Success

1. Deeply technical and competent resources are available to fully support the Partnership's application environment throughout the contract period.
2. Proactively monitor all application and system resources.
3. No unplanned outages due to application misconfiguration error(s) or human error.
4. A commitment to continuous quality improvement and following industry best practices.
5. Application customizations and configurations that are fully shared and supported.
6. Processes and procedures for managing each application are fully shared and kept updated.

Requirements

D1 Application Licenses

The Proponent should manage all vendor relationships and as directed by the Partnership, software licensing and annual support agreements.
The Proponent should:

1. Create and maintain a software inventory library with version control, patch update information and alerts as to license renewal dates that is accurate at all times.

2. Provide a software inventory library and any other software information needed to Service Desk so entry can be made in the CMDB (configuration management database).

3. Provide a sixty (60) days advance notice to the Partnership for software license renewals so that the appropriate procurement process can be initiated.

D2 Application Monitoring

The Partnership requires the Proponent to proactively monitor application availability, performance and response time.

The Proponent should:

1. Track the number of users of all applications.

2. Conduct routine tests to ensure that all applications are functioning as required.

3. Monitor and address alerts with regards to the lack of application resources such as low cache, memory, disk space or CPU availability to ensure that all applications always have the necessary resources to function and perform efficiently and effectively.

4. Monitor all externally internet-accessible URLs and endpoints.

5. Triage, troubleshoot and fix any application alerts as they are received.

6. Respond to all critical and high level alerts 7/24 as required to maintain service levels and disaster recovery objectives.

7. Perform remote monitoring of the application environment for the purpose of verifying and auditing of the environment.

8. Provide alerts and monitoring reports to the Partnership.

D3 Application Upgrades

The Partnership's strategy is to minimize customization and to remain current on software releases to leverage "out-of-the-box" functionality.

The Proponent can assume that:

1. There will be one (1) Agresso application upgrade per year.

2. There will be one (1) EmpowerID application upgrade per year.

3. There will be two (2) SQL Server upgrades during the contract period.

4. There will be two (2) Active Directory upgrades during the contract period.

5. Windows and Linux patching will be performed monthly during the contract period.

The Proponent should:

1. Include price for the upgrade in the monthly maintenance portion of the contract along with the patching for bug and security fixes
    - Agresso

- EmpowerID
- Ceridian

2. Provide assistance to third-party vendors performing installation or maintenance services for the Partnership. This includes, but is not limited to:
   - Dynamics CRM
   - OncoSim platform
   - Active Strategy
   - Digital agency of record

D4 Custom Application Support

Support requirements for the Partnership's custom applications such as the Canadian Clinical Trials and OncoSim platform are as follows:

The Proponent should:

1. Conduct analysis to identify the cause of application error (i.e. determine if the custom application is at fault for the error).

2. Review the server/application logs to verify if the error is being caused by the custom application or a result of an underlying hardware/software platform not functioning correctly.

3. Create an Incident and escalate it to the appropriate Tier 3 level resource(s) to address the issue, if the error is related to the underlying hardware/software platform.

4. Triage an Incident and escalate it to the Partnership for further investigation, if the error is related to the functionality within the custom application.

5. Ensure that the necessary logging is in place to support analysis and investigation to troubleshoot application errors.

For SQL server support, the Proponent should:

1. Provide general DBMS support (e.g., stop, start, backup/restore, user management) for environment.

2. Provide full DBMS support for all Microsoft server products (e.g., Dynamics CRM).

For MySQL/MariaDB server support, the Proponent should:

1. Provide general DBMS support for application environment (i.e., stop, start, backup/restore, user management).

D5 Modern Spam and Malware prevention

The Proponent should:

1. Provide application support for the Partnership's anti-spam and malware solutions.

2. Provide support for cloud based scanning and removal solutions.

D6 Virus Protection

The Proponent should:

1. Ensure that all hardware and software infrastructure is protected at all times by keeping the solutions up to date.

2. Provide support for the Partnership's antivirus desktop product (McAfee Endpoint Protection managed via McAfee ePO).

D7 Patch Management

The Proponent should:

1. Conduct ongoing discovery of new patches, testing and implementation for full suite of applications and data at all times.

D8 Maintain Privileged Account Management Process

The Proponent should:

1. Work with the Partnership's IT team and maintain the privileged account management process for server administration utilizing Windows, Linux and industry best practices.

D9 Ongoing Application Development

Application and System configuration changes are needed on a regular basis. This work should be included in the ongoing maintenance portion of the contract.

The Proponent should:

1. Ensure that the Partnership's IT Service Manager is informed on the change and how it will affect the environment prior to implementation.

2. Ensure that the Service Desk is informed and aware of the changes that affect the support of end users of the environment prior to going live.

EXHIBIT E - Managed Hosting Requirements

Introduction

The main goal of this managed service is to provide stable operating environments that maximize uptime and performance of the Partnership's application stacks through the provision of proactive monitoring, maintenance and support.

The Partnership's datacenter infrastructure currently resides at Peer 1 Toronto East for Production, Peer 1 Downtown II (151 Front St.) for Development/Stage/Disaster Recovery. The Partnership prefers that its Production datacenter infrastructure continue to reside at Peer 1 Toronto East, but is open to using an alternative hosting facility chosen by the Proponent. The Partnership is currently in the process of shifting to use Microsoft Azure virtual private clouds (VPCs) to support extended compute, backup and disaster recovery initiatives. The Partnership plans to decommission the secondary datacenter infrastructure at Peer 1 Downtown II by March 2017.

Current state applications and hosted environments are outlined in **Exhibit A** along with the future hybrid environment configuration that the Partnership will be transitioning to starting in 2017.

It is the Partnership's expectation that all aspects of infrastructure management, service request, support, operational health and performance be included as requirements of this Schedule.

Definition of Success

1. Provision/maintain one data center for the Partnership's on premise environment and assume the management of the Partnership's existing Microsoft Azure cloud environment.

2. Ensure that there is no single point of failure in any provisioned hardware. Identify single points of failure in access and present the dollar value associated with mitigating them in order for the Partnership to do a cost benefit analysis for the business.

3. Ensure that the physical security of the site is adequately provisioned to protect hardware, appliances, firewalls, applications and data stores from accidental or unauthorized physical access.

4. Ensure that logical security controls including preventive, detective, alerting and logging are robustly configured and tested to protect the Partnership's data from unauthorized access and malicious cyber-attacks.

5. Ensure that audit trails are adequately collected and protected. This should include audit trails such as physical access to the physical site, remote access to the site, authentication, network/firewall configuration changes, and access control changes which are essential ingredients for supporting incident management and forensic investigation.

6. Ensure that the service provider periodically conducts reliable vulnerability assessments on the network, server, data and physical infrastructure; and resulting reports are transparently shared with the Partnership.

7. Ensure that the performance of all of the Partnership's applications remains within a four (4) second acceptable time limit for a full loopback as defined in **Exhibit F, Section F4**.

8. Monitor, shape and actively manage bandwidth and QOS from the One University Ave. Office to the production data center, Azure private cloud and to the internet.

9. Proactively maintain and upgrade hardware/firmware to ensure that there are always ample resources i.e. memory, cache, disk space for the applications to run without error, downtime or quality of service issues. Focus on proactive health checks and automated system monitoring to prevent identifiable incidents and minimize the amount of reactive support required.

10. Receive all monitoring alerts from data centers, Partnership managed devices and infrastructure; and react according to the stated priority levels and their associated response times 7/24. Proactively monitor and manage all secure communication pipes that are connected to the One University Ave. Office

Requirements

E1 Data Center Space

The Service Provider should design, build and operate its own systems for continuous power and cooling distribution within its data centers. These systems should be engineered to operate each data center at 100% capacity with at least N+1 redundancy. Through a capacity reservation system, a dedicated portion of the capacity of these systems should be reserved for each customer.

E2 Site Security

Following is a set of requirements that the Partnership deems necessary to protect the data center from inadvertent and/or malicious access:

1. The data center should implement a multi-level security model including round-the-clock security guards, extensive video surveillance and biometric authentication.

2. Movement of equipment and personnel should be strictly controlled, both coming into and out of each data center.

3. Ensure that only authorized Proponent or Partnership staff are allowed physical access to the site and the physical infrastructure that the Proponent is managing for the Partnership's applications and data.

4. Each Service Provider should provide a recent copy of their SOC 2 and SOC 3 (Type 1 and Type 2) reports.

5. Each Service Provider should provide the ability for the Partnership to tour each facility if it so desires to witness firsthand the physical security elements in place. (REF: CSA 6.5)

6. TLS and IPSec should secure communication channels between servers and remote locations. Furthermore, it is the Partnership's requirement that its existing VPN infrastructure be extended for use in connecting to its resources within the hosted environments.

7. Audit trails pertaining to site access and control management should be maintained, backed up and available to the Partnership upon request.

E3 System Authentication/Identity and Access Management (Ref: CSA 6.9)

Provide holistic network device and server management that can automate password changes and enforce network security policies aligned with the risks and compliance outlined by the Partnership. The authentication and access control framework needs to cross application boundaries. It will need to be serviced and supported as an integral part of the contract. In addition:

1. Ensure that web connections utilize TLS 1.1 or 1.2 (or newer) and that inferior versions of the protocols are disabled;

2. The Proponent should demonstrate that they have the capability to generate audit trail reports for access control-related events. At a minimum, the reports should include information showing:

    a. Who had access to what system, when and for what purpose
    b. Who had access to the physical facility, when and for what purpose
    c. Who made changes to access control rules and policies, when and for what purpose
    d. Successful logins
    e. Failed logins

3. Considering the sensitivity and potential damage that can be impacted from the VM hypervisor or VPC management portal, the Partnership requires that the Proponent and the Partnership will jointly administer authentication and access control management to the hypervisor and VPC management portal. The Proponent is thus requested to propose methods, and alternatives as to how they envisage fulfilling this requirement.

E4 Network Uptime

99.99% uptime is required. The network should be fully redundant and designed to eliminate any single points of failure. The network should minimize delays and points of failure by using private connections where possible to avoid congested public Network Access Points. The data center should be available 100% of the time excluding planned maintenance. The Partnership is eligible for a credit for network downtime for any breach of this guarantee. Network downtime is defined as an inability to transmit and receive data caused by failure of network equipment managed and owned

by the data center excluding planned maintenance but including managed switches, routers and cabling.

E5 Network Monitoring

Monitor, shape and actively manage bandwidth between One University Avenue office, the production data center, Azure VPC, Partnership partners connected with dedicated links (e.g., Igloo, VOIP Telephony), and the Internet. Monitoring and reporting of real time bandwidth and quality of service with 7/24 automatic alert notifications is required. Monitoring and reporting function will include:

1. Core and edge device availability monitoring

2. Performance monitoring of firewall and network hardware/services with timely communication about performance problems or concerns with suggested resolution paths

3. Log monitoring, analysis and archival

E6 Configuration Control and Change Management

Operating system patching and upgrading is required. Rapid replacement services in the event of a hardware failure should be provided. 7/24 onsite management and support is required. In addition:

1. The Proponent should maintain audit trails to establish service offerings continue to meet what the Partnership needs.

2. The Proponent should maintain audit trails that substantiate change requests and maintenance and upgrade work affecting the network, server, storage and appliance infrastructure that have an impact on the Partnership's applications' performance metrics and availability.

3. Indicate a need to be able to gather and review these reports from provider in both a formal report from the provider as well as a capability to poll logs independently.

E7 System Availability

99.9% uptime excluding planned maintenance is a requirement. The measurement of availability of all software and infrastructure including the response times and accessibility of the application stack is a requirement. Trending data on this information should be kept and reported on in the trending report. Business critical services such as external online properties, email and the Partnership's enterprise resource planning system (Agresso) should be configured as high availability environments. Baseline performance measurements should be made for all internal system points of failure or bottlenecks. Performance tests should be run proactively and reported on a monthly basis to ensure that availability is within the four (4) second acceptable time limit for a full loopback for 99.9% of the reporting period. This is defined as from the time the end user presses enter / clicks on application icon until the application appears on the desktop. One further second to a total of (5) five seconds should result in the entire application being loaded and ready for use by the end user.

E8 Hardware Replacement

The Proponent should guarantee the functioning of all hardware, including servers, CPU's, cabling and associated server hardware, firewalls, load balancers, network appliance, storage area networks, and will replace any failed component at no cost to the Partnership within four hours following the Proponent's receipt of incident concerning the hardware issue and the Proponent's identification of the failed hardware. "Hardware" means the Processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware listed in the Service. The Replacement Guarantee does not include the time required to rebuild a RAID array or the reload of the operating systems and applications or changes to hardware during Maintenance.

E9 Managed Hardware

The Proponent is expected to commit to:

1. Managing and processing renewal of all support agreements covering hardware and software related to the server hardware, firewalls, load balancers, network appliances, and storage area networks.

2. Software upgrades, patch management and device configuration maintenance.

3. Device configuration change management and auditing.

4. Maintain backups of device configurations.

5. Comprehensive reporting to the Partnership upon request.

E10 Managed Firewall

1. The Proponent is responsible for installation, configuration and ongoing support including firewall rules configuration, rapid replacement program in the case of hardware failure, 7/24 on site management and support

2. The Proponent is required to share firewall solutions that they implement to protect the Partnership's hosted data and applications as integral part of the proposal response to the RFP.

3. The Proponent maintains audit trails pertinent to firewall access controls, configuration changes and change requests substantiating the need, and benefits to such changes.

4. The Proponent is required to avail firewall audit trails to the Partnership upon request

5. It should be noted that the Proponent is expected to commit to:
    a. Rule-set validation, verification, tuning, and optimization
    b. Review of firewall policy and firewall security posture assessments

E11 Vulnerability Management

1. The Proponent should demonstrate that there is a vulnerability management program which is leveraged to continually manage vulnerabilities with a focus on:

    a. Early identification of vulnerabilities affecting all network and server infrastructure and appliances managed by the Proponent;

    b. Availability of vulnerability life-cycle for management process including identification, response, remediation, and record keeping of all vulnerabilities remediated or otherwise.

    c. Notification and alerting of affected clients should be part of the response process. It is expected that notification will occur immediately after vulnerability is discovered along with stipulation of next steps including remediation timeframe, and temporary stop-gap measures until such remediation is applied and tested successfully.

2. The Proponent should commit to allowing the Partnership to enter its spaces in order to perform technical VA scans independent of the Proponent's own effort in this respect.

3. The Proponent should provide upon request vulnerability updates for managed hardware and services.

E12 Managed Load Balancing

Optimization of application and internet performance to improve our online digital property and business service response times and reliability.

E13 Managed Backup and Restore

Scalable and reliable backup service and rapid replacement in the case of hardware failure, 7/24 on site management and support. The backup service should be able to customize the retention period to suit the Partnership's requirements and employ good file management best practices. The Proponent should ensure that all data requiring backup is backed up on a daily basis at minimum and sufficient to satisfy Recovery Time Objectives outlines in **Section E14**. Data should be proactively managed to ensure that unused, legacy data is archived for retrieval when needed leaving ample storage capacity for current data. The data backup and archival service should support the Partnership's Records Management Program.

Work with the Partnership on an archival strategy whereby data that has not been utilized over a set period of time will be archived and will not add to the daily and monthly cost of the backup solution. The archiving system should balance frequency of access, retrieval time, frequency of change versus the frequency of backup, and the cost of storage.

Two full successful backups are required before any software upgrade can occur. These backups should be fully verified even when indicated successful prior to performing upgrades.

Archiving should be activated for data that is no longer frequently accessed and in accordance with the Partnership's Records Management retention schedule. Duplicate data should be identified and proactively managed through end user education, formalized file naming conventions, technology and other processes as outlined in the Partnership's Records Management policy and procedures.

E14 Disaster Recovery

It is essential that the Partnership's IT Disaster Recovery Plan is maintained and continues to meet the Partnership's Recovery Time Objectives as specified in the Partnership's Business Continuity Plan.

Systems requiring restoration include, but are not limited to:

System	Function or Asset	Degree of Risk	Recovery Time Objective
Websites	Cancerview OncoSim Moodle Canadian Cancer Trials	Medium	2 days
Webservices	EmpowerID	High	1 day
Documents	Records Management Igloo Binary Server	High	1 day
Partner Website	Canadian Virtual Hospice (CVH)	High	1 day
Cisco VOIP	Telephone system	High	1 day
Network File System	File and Print	Medium	2 days
MS Dynamics CRM	Contact Management	Low	2 days
Applications	Agresso, Microsoft Office, e-mail, Active Directory, Ceridian	High	1 day
WebEx	Audio/Video Conferencing	Medium	2 days

Disaster Recovery Testing

The Proponent should:

1. Perform annual failover and failback testing of the Partnership's systems.

2. Ensure the data center and cloud service providers provide evidence or attestation that it has performed a disaster recovery test run at least once a year.

3. Ensure that the required data restoration and application activation cycle times meet the Partnership's Recovery Time Objectives.

Disaster Recovery Incident Response

In the event of a disaster-related incident, the Proponent should be able to perform:

1. After-hours response to system outages by on-call staff
2. Incident response related to disruptions of service from network or other related failures
3. Network, firewall, hardware and application fault analysis and provide timely problem resolution; and
4. Provide a formal report to the Partnership outlining incident cause and implemented remediation, or stopgap measures along with proposed action plan for implementing a final remediation measure.

Disaster Recovery Reporting

1. Architectural documentation should be up to date prior to the testing day and a fully documented DR test run should occur. Any ongoing changes throughout the year should be documented along with the corresponding effect on the disaster recovery plan. The disaster recovery procedures should be documented and kept up to date at all times and reviewed in full semi-annually.

2. A full report including deficiencies, and remediation plan and fixes should be produced. All testing should be timed from failover to production.

3. The Partnership will also be able to utilize an active/passive type BCP/DR capability in that on premise back-ups can be done and images sent to the cloud space for use in a disaster recovery situation. The only consideration here is that a Recovery Time Objective of 24 hrs would be required to stand-up operations in the cloud should on premise functionality be compromised. Once Recovery Time Objective elements were completed on premise there would need to be a 'draw-down' of services in the cloud back to on premise systems components.

4. The Partnership at any time may request the Proponent's contingency documentation for review and shot-check.

E15 DNS Management

The Proponent should perform domain name registration, renewal and management.

E16 VPN Management

The Proponent should provide a fully managed VPN for secure communication between the data center, Azure cloud and One University Avenue. The VPN service should be provisioned to support:

1. Site-to-site VPN connections, and
2. End-user VPN connections
3. Integration with the Partnership's own VPN solution.

E17 Managed Telephony

The Proponent should proactively support connectivity and quality of service for the Partnership VoIP solution and all unified communications solutions. The Partnership is currently using a Cisco Unified Communications Manager with Cisco IP phones, Cisco IP Communicator and Cisco Jabber. The Partnership is currently evaluating alternative technologies for unified communications and may be transitioning to another – potential hosted - platform prior to or during the contract period.

E18 Security Incident Management and Cloud Forensics

The Proponent should demonstrate that they have processes and systems in place to resolve incidents, malicious or otherwise including event monitoring and alerting, contact, triage, resolution and post mortem; aspects constituting areas where pre-planning brings value in terms of timely response, resolution and lessons learned. The Proponent should also demonstrate:

1. That there is a tested and repeatable incident response and resolution procedure in place.
2. That they have catalogued what constitutes major incidents and factors influencing such categorization.
3. Ability and processes to report in a timely fashion and to the right "audience" an incident and/or security incident or breach
4. How incidents are escalated and up to what level within the Proponent organization and customer audience
5. Expectation is that the Proponent possesses automatic messaging system and templates for repeatable and immediate use (i.e. issue ticketing system). In such case, the Proponent should submit with the RFP response such templates indicating how each is used and for addressing what audience (e.g. Incident response resolver, IT department head, executives, direct stakeholders, etc.…)
6. The availability of the messaging system to communicate incident alerts and escalation processes and updates is critical. The Proponent should demonstrate how available their electronic infrastructure and what alternatives they put in place to protect from accidental failure in order to ensure reliable incident communications.
7. The Proponent should provide a description of the technologies, relevant training and business processes that they have in place in support of their adopted incident response strategy, e.g. CSIRT process.
8. The Proponent should specify how their audit trails are collected, relevant data sources, how frequently it is backed up, and for how long it is retained.

E19 Audit Support

The Proponent should have the capability for auditing of actions affecting resources (physical and logical) dedicated to supporting the Partnership's hosted data and applications.

1. The Service Provider should demonstrate independent auditing of its environment using a third party and alignment/compliance with accepted industry best practices. Initial standards would be the CSA CCM self-assessment as a starting point to demonstrate compliance to standards such as PIPEDA, Privacy Act, SOC 2 and SOC 3, ISO 27001 and ITSG-33 (NIST 800-53 equivalent) controls, ISO 23001, etc.

2. The Partnership requires that third party auditors are asked to submit copies of their reports to the Partnership. It is acknowledged that entry into an NDA to accept this information may be required.

3. The Proponent should provide a description of existing technical, training and staffing infrastructure in support of performing audit functions, albeit conducted internally or by 3rd party auditors.

4. The Proponent should describe how often IT Audits are performed, including the scope and breadth of the audit. The date of the most recently conducted audit should be provided along with audit objectives and report title.

E20 Encryption and Key Management

Following are the Partnership's requirement for the use of encryption for protecting data security, both when at rest and in transit:

1. The Service Provider will allow the Partnership to use its own encryption schemes and that the Partnership will maintain the keys at its own site.

2. A description of Service Provider's available encryption scheme should be included for consideration.

3. All encryption should meet acceptable bit strengths. Refer to CSE ITSB-111 (or newer) as a GC standard for benchmarking.

4. Database encryption should be allowed for database structures and data being housed in virtual machines or network mounts. Encryption at the file level should be allowed where deemed necessary.

E21 Governance and Risk Management

1. The Proponent should be able to demonstrate the availability of, and adherence to an adopted Program Management and Reporting process, including frequency of conducting reviews of the

Program Management regime in place and undertaken measures to remediate identified gaps that affect the quality of service rendered to the Partnership.

2. The Proponent should indicate whether a maturity assessment has ever been conducted, the frequency at which the assessment is conducted, number of times and date of the most recent assessment.

3. The Proponent should demonstrate that they have implemented an enterprise risk management (ERM) strategy/policy and efforts to enforce the tenets of the policy are underway.

E22 Assessments

As directed by the Partnership throughout the contract period, the Prponent will participate in privacy impact assessment and threat risk assessments, policy reviews, maturity assessments that are commissioned by the Partnership. Work collaboratively with the Partnership to develop and execute action plans to mitigate risk. The Proponet will resolve vulnerabilities, process gaps and issues identified from any assessment.

EXHIBIT F - Service Level Objective (SLO) Requirements

Introduction

The Service Level Objectives in this Exhibit should be reviewed on a regular basis throughout the contract period. As part of the review, performance trends should be normalized and reviewed to determine sources of any deficiencies. An SLO action plan will be created to resolve any gaps from the review. As part of the SLO action plan, the Partnership and the Proponent will consider revising existing and/or introducing new metrics and Service Level Objectives in keeping with the objective of continuous improvement.

There may be additional KPIs that need metrics and reporting but have no formal Service Level Objective.

Requirements

F1 Service Desk Objectives

Service Level Objectives set below are based on historical trends and should be reviewed and revised based on the SLO Review Process.

The service desk should meet the following minimum Service Level Oobjectives for each of the stated service elements:

Metric	Service Level Objective
Calls answered <= 30 seconds **(Length of time call rings until answered)**	>80%
Incident number assigned <= 30 minutes **(Incident number given to customer within 30 minutes of them sending the request)**	>80%
Call Abandonment Rate **(Caller hangs up call prior to call being answered by service desk)**	<5%
Duration of first call < 15 minutes **(Callers should not be kept on the phone for longer than 15 minutes)**	>90%
First call resolution rate	>60%

(Defined as the number of incidents solved after the first call in to the service desk and within 15 minutes of triage and troubleshooting)	
First Level Resolution Rate (Defined as number of Incidents resolved without escalation to Tier 2 / Tier 3 resources) and within 1 business day of first call	>80%
Incidents categorized and routed correctly	>90%
Customer Satisfaction **(Defined as the total of Satisfied + Very Satisfied divided by the total number of surveys received)**	>90%

F2. Incident Management Service Level Objectives

Incident Management (as part of the Service Desk or a separate team) should meet the following minimum service level objectives for each of the stated service elements:

Metric	**Service Level Objective**
Mean Time to Repair <= 4 hours **(Average time between incident detection and final resolution)**	>90%
Mean Time to Detect <= 2 hours **(Average time between an Incident causing event and detection by the Service Desk or Tier 2)**	>90%
Incidents handled within SLA	>90%
Repeat Incidents **(Re-occurring incidents that have the same issue and resolution)**	<20%
Reopened Incidents **(Closed incidents that need to be reopened because resolution wasn't accepted by users)**	<10%
Overdue Incidents	<10%

(Ongoing Incidents without resolutions that won't be resolved within SLA)	
Incidents Resolved before user interaction	>50%
Unresolved Incidents	<10%

F3. Managed Hosting Objectives

If an unplanned outage specifically related to the hosted data center or the One University physical facilities occurs, the following recovery time objectives should be achieved:

System	Function or Asset	Degree of Risk	Recovery Time Objective
Websites	Cancerview OncoSim Moodle Canadian Cancer Trials	Medium	2 days
Webservices	EmpowerID	High	1 day
Documents	Records Management Igloo Binary Server	High	1 day
Partner Website	Canadian Virtual Hospice (CVH)	High	1 day
Cisco VOIP	Telephone system	High	1 day
Network File System	File and Print	Medium	2 days
MS Dynamics	Contact Management	Low	2 days
Applications	Agresso, Microsoft Office, e-mail, Active Directory, Ceridian	High	1 day
WebEx	Audio/Video Conferencing	Medium	2 days

F4. Application Management Objectives

Metric	Service Level Objective
Application Performance	4 seconds

(Length of time from when end user presses enter / clicks on application icon until the application is loaded and ready for use by the end user)	

F5. Outage Definitions for Fee Abatement

In cases where the Proponent fails to meet the minimum Service Level Objective, financial fee abatements may apply based on the definitions detailed below;

Minor Unplanned Production Environment Outage:

a) Low and medium priority incident falls outside of the Service Level Objective for more than one (1) business day at anytime

a) Service Desk produces customer satisfaction ratings that fall below 90%

Major Unplanned Production Environment Outage:

a) Specific application functionality is inaccessible at any time

b) Managed Hosted Environment is inaccessible

c) Service Desk is unavailable via phone, e-mail or web

d) Critical to High priority Incident falls outside of the Service Level Objective for more than two (2) hours at anytime

e) Service Desk produces customer satisfaction ratings that fall below 80%.

Metric:

1) One (1) minor unplanned production environment outage is permissible per quarter. One minor outage is defined as fifteen minutes (15) of a Priority 3 or 4 incident during the business hours of 8 – 6 pm Monday – Friday. Two minor outages per quarter = One major outage

2) One (1) major unplanned production environment outage is permissible per quarter. One major outage is defined as one hour (1) of downtime of any mission critical or high priority system during the business hours of 8 – 6 pm Monday – Friday. For the service desk environment, satisfaction ratings falling below 80% once per quarter is defined as a major outage.

3) Greater than four (4) major outages in one twelve month timeframe will result in written notice of non-performance from the Partnership. Written notice of non-performance will

happen only once in one twelve month rolling timeframe giving the proponent the ability and notice to remedy.

4) Greater than four (4) major outages in one twelve month rolling timeframe will allow the Partnership to withdraw from the contract without penalty.

EXHIBIT G – Terms and Conditions of the Agreement

Letter of Agreement - Term Sheet (LOA- TS) for IT Solution

[signing authority and Supplier entity/address]

Dear [name]:

Re: Letter of Agreement - Term Sheet (LOA-TS) in respect of IT Solution

This Letter of Agreement - Term Sheet (LOA-TS) (the "Letter of Agreement - Term Sheet (LOA-TS)") dated [DATE] (the "Effective Date") is intended to generally describe the fundamental business terms for the proposed [hosting], licensing, implementation (including configuration and training), and ongoing maintenance and support of an information technology system ("IT Solution") by ["x"] ("Supplier") to Canadian Partnership Against Cancer Corporation ("Partnership"). On the basis of this LOA-TS, a definitive agreement between the parties can be prepared and negotiated. No party shall have any legal obligation or liability in respect of Section 1 below to the other unless and until the applicable definitive agreements (the "Definitive Agreement(s)", as further defined in Section 1 below) are executed by duly authorized representatives of each party. To the extent that a party incurs expenses or liabilities in reliance on negotiating the Definitive Agreement, it does so at its own risk in the event the Definitive Agreement is not executed.

The parties agree as follows:

1. **Form and Timing of Definitive Agreement.** The parties shall endeavour to negotiate the Definitive Agreement that shall include, in substantial form, those terms and conditions set out in Schedule "A" (the "Letter of Agreement - Term Sheet (LOA-TS)") to this Letter of Agreement - Term Sheet (LOA-TS). The Partnership shall prepare the first draft of the Definitive Agreement within ["x"] days of the Effective Date. The parties agree to negotiate in good faith to finalize the Definitive Agreement within ["x"] days from the date the Partnership provides Supplier with the first draft.

Upon mutual agreement, Supplier shall bring to the Partnership's location (as reasonably required), its personnel with the authority to finalize the negotiation of all material terms to the Definitive Agreement. Either party may terminate negotiations at any time prior to the execution of the Definitive Agreement on notice to the other party.

2. **Publicity.** No party shall make any public statement or issue any press release concerning the Letter of Agreement - Term Sheet (LOA-TS), the Definitive Agreement or the fact that negotiations are taking place without the consent of the other party, except as may be necessary, in the opinion of counsel, to comply with the requirements of applicable law. If any such public statement or release is so required, the party making such disclosure shall, to the extent practicable, consult with the other party prior to making such statement or release and each party shall use all reasonable efforts, acting in good faith, to agree upon the text of such statement or release. If a party is subject to a legal requirement to make disclosure, that party shall have the final determination as to the timing and content of such disclosure.

3. **Confidentiality.** Each party agrees to use the same degree of care to protect the confidentiality and security of any documents, materials and information which by their nature ought to be treated as confidential and which belong the other parties ("Confidential Information") from disclosure to third parties as it uses to protect its own Confidential Information of similar importance (but in no event less than reasonable care). Disclosure of this Letter of Agreement - Term Sheet (LOA-TS) shall be restricted, in respect of The Partnership and the Supplier, to their: (i) professional advisors and (ii) employees, each of whom to have a need to know. No party will be required to keep confidential any Confidential Information that is publicly available without a breach of this Letter of Agreement - Term Sheet (LOA-

TS); is lawfully obtained by one of the parties from any third party having legitimate possession of the information disclosed and the right to make such disclosure; or is disclosed by legal requirement, provided that the receiving party provides the disclosing party with reasonable notice of such requirement in order to permit the disclosing party to object to or seek an appropriate order to prevent or limit such disclosure. In the event of the termination of this Letter of Agreement - Term Sheet (LOA-TS), the Confidential Information shared under this Letter of Agreement - Term Sheet (LOA-TS) shall be returned to the disclosing party, or disposed of by a method acceptable to the disclosing party. Each party shall send a letter to the other confirming that the disposal has been done in the agreed manner.

4. **Own Expenses.** The parties shall each be responsible for their own respective costs incurred in connection with the negotiation and entry into of this Letter of Agreement - Term Sheet (LOA-TS) and the Definitive Agreement, including any obligations that such parties may have incurred or otherwise agreed to assume for any finder, consultant, broker or agent in respect of this Letter of Agreement - Term Sheet (LOA-TS) or the Definitive Agreement.

5. **Applicable Law.** This Letter of Agreement - Term Sheet (LOA-TS) shall be interpreted, construed, and governed by and in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein (other than any conflict of law rules that would result in the choice of laws of another jurisdiction) and shall be treated, in all respects, as an Ontario contract. The parties agree to submit to the non-exclusive jurisdiction of the courts of Ontario. The parties expressly exclude the application of the United Nations Convention on Contracts for the International Sale of Goods.

6. **Survival.** Sections 2 through 6 shall survive the termination of this Letter of Agreement - Term Sheet (LOA-TS) and the failure or success of the parties to negotiate the Definitive Agreements, unless specifically amended in the Definitive Agreement.

Yours truly,

CANADIAN PARTNERSHIP AGAINST CANCER CORPORATION

By: _____

The terms set out in this Letter of Agreement - Term Sheet (LOA-TS) are accepted with effect as of the Effective Date by Supplier as evidenced below.

[SUPPLIER]

By: _____

SCHEDULE "A"

LETTER OF AGREEMENT – TERM SHEET (LOA-TS)

A. General Terms of the Definitive Agreement

1. **Orderly and Timely Implementation.** The orderly and timely implementation of the IT Solution is of necessary to the Partnership and shall form a fundamental term of the Definitive Agreement. Orderly and timely implementation is a joint effort that requires the focus and cooperation of all parties and their respective suppliers and agents. Supplier acknowledges the requirement to apply appropriate resources in a timely manner that is consistent with the implementation schedule mutually agreed to by the parties, and also considering that the Partnership may implement the overall IT Solution in multiple phases over time. The Partnership may elect to have specific Supplier personnel involved in the implementation replaced at Partnership's discretion, acting reasonably, and Supplier shall apply appropriate resources to ensure a timely seamless transition in such circumstances.

2. **Ownership and License of Products.** In respect of the IT Solution, Supplier grants to the Partnership a perpetual, fully-paid up license that shall permit the use of such IT Solution for the purposes reasonably contemplated by this Agreement. The Partnership may have the IT Solution hosted on its behalf by a third party that agrees to abide by the confidentiality provisions agreed to by the Partnership.

3. **Approval Testing.** At the Partnership's request, a specific acceptance testing procedure acceptable to the Partnership and the Supplier will apply that will provide the Partnership with a reasonable period of time to confirm material conformance of the IT Solution with the specifications (including functionality, speed, uptime, interoperability and scalability) provided for in the Supplier's Proposal, in all material respects in a production environment. Such testing may occur in phases to reflect the implementation of the applicable deliverables as part of a system. In respect of acceptance testing, a failure of the IT Solution to successfully pass acceptance testing, within ninety (90) days from the initial start of acceptance testing, will allow the Partnership to terminate the Definitive Agreement for cause and to receive a refund of all amounts paid under the Definitive Agreement.

4. **Maintenance Term.** Subject to early termination for cause and the right of extension by the Partnership for transition, the maintenance and support services for the IT Solution will be available at the Partnership's request, on a year by year basis, for the term of the Definitive Agreement, and including any Transition on Termination provision.

5. **Transition on Termination.** Following termination, the Partnership may extend the Agreement by up to two (2) years immediately following termination (for cause by either party) to assist in transitioning to a new supplier and the Partnership will pay the Supplier reasonable fees (being the fees in the Agreement, or in the absence of the applicable fee, at the Supplier's then standard published rates) for its services performed during any such transition period. The Partnership will have a perpetual right to use the pre-existing deliverables on termination provided that the license to use the preexisting deliverables has been paid for and termination is unrelated to a continuing and intentional action by the Partnership to violate the intellectual property rights of the Supplier in the IT Solution.

6. **Warranties.** Warranties will be provided by Supplier as to skill of staff and standard to which deliverables will perform as part of the overall IT Solution. A warranty will be provided by Supplier as to the sufficiency of any applicable third party components to be compatible and sufficient to meet the specifications set out in the Proposal or such other standard negotiated by the parties. Deliverables to be provided without encumbrances and otherwise to be appropriate to perform to the applicable standard provided for in the Definitive Agreement, including

applicable regulatory standards consistent with their reasonably contemplated use under the Definitive Agreement. The warranties and remedies provided shall apply equally to the entire IT Solution, including third party components, and shall continue to apply for so long as the Partnership subscribes for ongoing maintenance and support services. Also warranties as to the provision of virus-free software, the adequacy of applicable source code materials for their contemplated use by the Partnership, and the conformance of all services and other deliverables with applicable law, will be provided by the Supplier. Subject to the Partnership conforming to applicable hardware requirements, there will be a warranty as to the limit of scalability of the IT Solution that is consistent with the other performance and functional specifications of the IT Solution.

7. **Limitation of Liability.** The parties agree to a limitation of liability provision that will only exclude, as to types of damages, a party's right to consequential damages in the nature of loss of profits or loss of revenue and will limit the quantum of damages that are cumulatively available from the other party to the greater of: (i) the amount paid under the Definitive Agreement; and (ii) ten (10) million dollars. Exceptions to any limit on any type or quantum of liability will be provided for (i) breach of confidentiality obligations; (ii) breach of privacy provisions; (iii) damage to tangible or real property or injury or death to persons due to negligence; (iv) intentional misconduct; (v) breach of applicable law; and (vi) the intellectual property indemnity.

8. **Intellectual Property Indemnity.** The Partnership will be held harmless from damages suffered from, and defended by the Supplier, in respect of, any third party intellectual property claim respecting the use of the deliverables provided by Supplier and in the manner contemplated by the Definitive Agreement. Subject to a court injunction binding upon the parties in Ontario that cannot be removed through the best efforts of the Supplier, in all events of intellectual property infringement asserted in respect of the IT Solution, Supplier shall allow the Partnership an additional minimum two year period to continue to use and to migrate to an alternative solution while maintaining the foregoing intellectual property indemnity in respect of such continued use.

9. **Termination for Cause.** In respect of material breaches, the breaching party will have a sixty (60) day period to correct the breach after notice thereof after which the non-breaching party can terminate immediately on notice. Material breaches can include a series of otherwise non-material breaches of key service level agreements that, over a period of time, culminate into a material breach for which notice can be provided.

10. **SLAs.** Mutually agreed SLAs will be attached to the Definitive Agreement to measure all material forms of performance against specific standards. There will be set-offs against the fees on a prospective basis for a failure to meet the SLAs of a range of 5% (going to 10% for a quarter to quarter failure to meet the 5% SLA) to 25% of the applicable maintenance fees as well as a right to terminate if a recurring failure is a material breach of the Definitive Agreement and it is not corrected within the applicable period of time. Both uptime and response times are of fundamental importance. The hardware and associated components that will provide the required sub-second response time to ensure optimal performance and reliability will be mutually agreed upon by Supplier and hardware/network provider and described in this TS-LOA and thereafter in the Definitive Agreement. Supplier's SLA in this respect is limited only to performance "within the box", ie application and database configuration, unless hosting services are provided by Supplier, in which event such elements shall also be incorporated into the SLAs. Schedule "B" includes details on uptime and response time requirements.

11. **Security and Confidentiality.** The Partnership is subject to privacy requirements, and the Supplier shall at all times comply strictly with the Definitive Agreement in such manner as to ensure that its acts or omissions do not result in the Partnership being in violation of any applicable privacy requirements. No ownership rights in any information or data that the Supplier may have access to by virtue of the Definitive Agreement shall accrue to the Supplier. Schedule "C" shall be used in respect of the privacy provisions. Supplier will provide reasonable co-operation and

assistance in the conduct of privacy impact assessments and threat risk assessments by the Partnership.

12. **Law.** Laws of Ontario and the exclusive forum of Ontario courts to apply. Either party can terminate for cause without the obligation to engage in dispute resolution, mediation or arbitration.

13. **Management and Reporting.** There is to be a process to facilitate rapid notice of failure to conform to the SLAs and to the other terms of the Definitive Agreement and to discuss and resolve such failures.

14. **Payments.** The Partnership may withhold payments on deliverables that are not satisfactorily performed, and payments shall be made on the basis of mutually agreed milestones and not on the mere passage of time.

15. **Proposal Documentation.** At the Partnership's request, all proposal documentation presented by the Supplier, to the extent still applicable to the value proposition proposed by the Supplier, shall be incorporated into the Definitive Agreement.

16. **No Indemnity.** The Supplier will not be seeking an indemnity from the Partnership.

17. **Indemnity from Supplier.** The Supplier shall provide an indemnity, and have in place appropriate insurance, for injury or death to persons or damage to tangible or real property resulting from the negligence of Supplier or product liability claims respecting the IT Solution. The Supplier acknowledges that it, he or she, is not an employee, servant or agent of the Partnership or the Minister and will not represent or hold itself, himself or herself, out to third parties in that capacity. To the extent that any third party, in reliance upon representations by the Supplier, considers the Supplier to be an agent or employee of the Partnership, the Supplier indemnifies the Partnership for any loss or damages and costs occasioned thereby by such third party.

18. **Audit.** During the term of the Definitive Agreement and for two (2) years after the expiration or termination of the Definitive Agreement, the Partnership shall have the right, but not the obligation, to perform financial and security audits of the selected Supplier in relation to the selected Supplier's performance and the invoicing of same.

19. **Recitals.** There shall be detailed recitals that set out the fundamental aspects of the relationship as a part of the Definitive Agreement including the following:

    a) The funding for this Definitive Agreement provided by the Partnership is, in whole or in part, obtained pursuant to a funding agreement (the "Health Canada Funding Agreement") between the Partnership and Her Majesty the Queen in Right of Canada as represented by the Minister of Health (the "Minister");

    b) The Health Canada Funding Agreement requires the Partnership to require certain minimum terms and conditions in agreements; and

    c) The Supplier acknowledges the source of the funding and recognizes the need to ensure that there is a high level of accountability and transparency in the receipt and expenditure of the funding.

20. **Force Majeure.** There will be a provision excusing performance for events beyond the reasonable control of a party applying reasonable foresight and due diligence provided: (i) prompt notice is provided of the event; (ii) a workaround strategy is promptly developed; and (ii) all commercially reasonable efforts are used to provide a work-around and to otherwise resume service to the applicable standard. A failure by a subcontractor or agent to perform

shall not be an event of force majeure for a party, unless the subcontractor or agent has itself experienced an event of force majeure. Labour disputes or lock-outs suffered or caused by a Party or its subcontractors or agents shall not be considered an event of force majeure. A requirement to disclose Personal Health Information other than under Canadian law pursuant to the terms of this Agreement shall not be an event of force majeure. The application of the force majeure provision shall be limited to 30 days.

21. **Escrow.** The Supplier will agree to a technology materials trust agreement for pre-existing materials. This agreement will permit access to and use of the Supplier's source code and other materials for the IT Solution. Such materials would be held by a third party trustee in Ontario. The materials would include those materials reasonably required to allow the Partnership to independently maintain and support the IT Solution. Release of the materials by the trustee would be triggered by the Supplier's failure to cure a material breach of its Solution-related maintenance obligations or to otherwise make maintenance and support services available.

22. **Novation.** On a minimum of sixty (60) days' prior written notice describing the particulars thereof, the Partnership shall have the right to novate its respective rights and obligations to a new corporation or other entity created to operate the IT Solution.

23. **Appropriation**. Payment under the Definitive Agreement at any given time is subject to the Partnership having been provided funding from the Minister of Health for the service for the fiscal year in which payment is due.

24. **Conflict of Interest.** Supplier declares that it has no interest in the business of any third party that would cause a conflict of interest or seem to cause a conflict of interest in performing the IT Solution. Should such an interest be acquired during the term of the Definitive Agreement, Supplier shall declare it immediately to the Partnership. It is a term of the Definitive Agreement that no individual, for whom the post-employment provisions of the Conflict of Interest and Post-Employment Code for Public Office Holders or the Conflict of Interest and Post-Employment Code for the Public Service apply, shall derive a direct benefit from the Definitive Agreement unless that individual is in compliance with the applicable post-employment provisions.

25. **Incapacity to Contract.** Supplier certifies that it and its officers, agents and employees are not prohibited under subsection 750(3) of the Criminal Code from benefiting from a government contract.

26. **Members of the House of Commons.** No member of the House of Commons or the Senate shall be admitted to any share or part of the Definitive Agreement or to any benefit to arise therefrom.

27. **No Bribe.** Supplier represents and covenants that no bribe, gift, or other inducement has been or will be paid, given, promised or offered directly or indirectly to any official or employee of the Partnership or to a member of the family of such a person, with a view to influencing the entry into the Definitive Agreement or the administration of the Definitive Agreement.

28. **Proactive Disclosure.** Information contained in the Definitive Agreement in relation to the following data elements – proponent name, reference number, effective date, description of the IT Solution, term of the Definitive Agreement, and total Definitive Agreement value may be gathered and may be posted to the Partnership's website. Information that would normally withheld under the *Access to Information Act* and *Privacy Act* will not appear on the website. This public disclosure is intended to ensure that the Definitive Agreement information is collected and presented in a manner that promotes transparency and facilitates public access.

29. **Accounts and Audit**

a) In addition to Section 18 (Audit), the Supplier shall keep proper accounts and records of the cost to the Supplier of the IT Solution and of all expenditures or commitments made by the Supplier in connection therewith, and shall keep all invoices, receipts and vouchers relating

thereto. The Supplier shall not, without the prior written consent of the Partnership, dispose of any such accounts, records, invoices, receipts or vouchers until the expiration of six (6) years after final payment under this Definitive Agreement, or until the settlement of all outstanding claims and disputes, whichever is later.

b) All such accounts and records as well as any invoices, receipts and vouchers shall at all times during the retention period referred to in sub-section a) be open to audit, inspection and examination by the authorized representatives of the Partnership, the Minister or the Auditor General of Canada, who may make copies and take extracts thereof. The Supplier shall provide all facilities for such audits and inspections and shall furnish all such information as the representatives of the Partnership may from time to time require with respect to such accounts, records, invoices, receipts and vouchers.

30. **Changes**

a) If, on the basis of progress reports provided to the Partnership or for any other reason, the Partnership and the Supplier decide that modifications to the IT Solution or modifications to line items within the budget are needed, the appropriate changes may be made by the administrative contact for the Partnership and the Supplier provided that no increase shall be made to the maximum amount payable hereunder and further provided that no other term of the Definitive Agreement may be altered in this fashion.

b) If the change is greater than 15% or $50,000 of the maximum amount payable, whichever is lesser, or if the maximum amount payable changes, the formal addendum process, signed by the approved delegated authority, shall apply.

31. **Communications**

a) In the event that the Definitive Agreement requires work with members of the public, the Supplier shall take the necessary measures to respect the spirit and intent of the Official Languages Act to communicate with the public in the official language (i.e., English or French) of their choice;

b) Any person, including individual researchers, related to the Supplier shall ensure that, as appropriate, announcements, services, documents, conferences, meetings, workshops, etc., be in both official languages, that community members of both official languages be encouraged to participate in its activities, projects or programs and that its activities, projects or programs will meet the needs of the two linguistic communities.

B. Pricing and Payment Milestones

1. Pricing and Price Milestones. The pricing and price milestones in Exhibit XX [not included] shall apply. No term of the Definitive Agreement or this Letter of Agreement - Term Sheet (LOA-TS) (including this Letter of Agreement - Term Sheet (LOA-TS)) shall be interpreted or applied in a manner inconsistent with the BPS Expense Directive, which directive shall be paramount in all circumstances, with respect to the reimbursement of expenses to Supplier.

C. Specific Terms Respecting IT Solution

1. Integration Specifics. [To be addressed in negotiations]

2. Network Availability. [To be addressed in negotiations]

3. Technical Requirements [To be addressed in negotiations]

4. Hosting Services. Among other provisions, if the Supplier is providing Hosting Services, it agrees to conform to the security provisions in Schedule "D".

Schedule "B"

UPTIME AND RESPONSE TIME REQUIREMENTS

To be consistent with Supplier's response to the RFP SLAs.

Schedule "C": Proposed Letter of Agreement - Term Sheet (LOA-TS)

PRIVACY PROVISIONS

Definitions and Interpretation

1. In this Schedule, the following terms have the following meanings and any capitalized terms that are not defined in this Schedule "C" have the meaning attributed to them in the Agreement:

(a) "access" in connection with Personal Data, means to have access whether or not the Personal Data is actually read, reviewed, scanned, copied or otherwise used;

(b) "Authorized Personnel" has the meaning attributed thereto in section 8(c) below;

(c) "Contact Information" means the name of a person (when used in his or her capacity as an employee, independent contractor, officer or director of the Partnership) and the person's position or title, business address, business telephone number, and any other information that is from time to time excluded from the definition of "personal information" in the *Personal Information Protection and Electronic Documents Act* (Canada);

(d) "Supplier Privacy Requirements" means the obligations of and the restrictions and prohibitions applicable to the Supplier in regard to Personal Data set out in this Schedule "C" and in any privacy law applicable to Supplier in its capacity as a service provider to the Partnership;

(e) "Personal Data" means collectively, "Personal Information" and "Personal Health Information";

(f) "Personal Health Information" means information to which Supplier has access as a function of providing the IT Solution that identifies an individual and relates to: his or her physical or mental health, including the health history of the individual's family; the providing of health care to the individual, including the identity of his or her health care providers, substitute decision-makers and health numbers; payments or eligibility for health care or health care coverage; and the donation of a body part or bodily substance, or the testing or examination thereof;

(g) "Personal Information" means information to which Supplier has access as a function of providing the Hosted and Services Solution that identifies an individual, but does not include Contact Information; and

(h) "use" in connection with Personal Data means to handle Personal Data in any manner, including to copy, download and hold Personal Data, but excludes the de-identification of Personal Data.

2. References to Supplier include its employees and agents, including permitted subcontractors, unless otherwise provided.

Relationship of the Parties

3. The Partnership is the provider of Cancer View Canada, an Internet-based portal environment that among other services, provides electronic means for individuals to collect, use, disclose and retain Personal Data and also operates certain back office systems containing Personal Data applicable to its operations.

4. Supplier is a service provider retained under this Agreement to assist the Partnership in connection with Cancer View Canada by providing the IT Solution.

5. Supplier is responsible for the acts and omissions of Authorized Personnel in regard to Personal Data.

6. Nothing in this Agreement will be construed to grant Supplier any custody, control, title or rights or interest in or to Personal Data.

Restricted Use of Personal Data

7. Supplier acknowledges and agrees that it will be necessary for Supplier to access, use, hold, store and transfer Personal Data to provide the IT Solution.

8. In providing the IT Solution, Supplier will comply with the Supplier Privacy Requirements and without limiting the generality of the preceding, Supplier will:

(a) only access and use Personal Data as necessary to provide the IT Solution and will not access or use Personal Data for any other purpose or on its own behalf;

(b) not disclose Personal Data to any person or organization including without limitation, to an affiliated third party;

(c) not permit its employees or any person acting on its behalf ("Authorized Personnel") to have access to Personal Data unless such access is required for Supplier to provide the IT Solution and unless Authorized Personnel agree to comply with all applicable Supplier Privacy Requirements.

9. For clarity, the access and use of Personal Data under this Schedule "C" by Authorized Personnel does not constitute a disclosure of such Personal Data by Supplier to Supplier Authorized Personnel.

10. Supplier acknowledges that information which is Confidential Information, as defined in the Agreement, may also be, but is not necessarily, Personal Data. Where information is Confidential Information and Personal Data, the requirements applicable to each type of information will apply to so as to subject the information in each case to the more rigorous requirement.

11. If Supplier receives any request for access to or the correction of Personal Data which it is holding or storing to provide the IT Solution, Supplier will promptly direct the request to the Partnership, provided, however, that nothing in this Schedule "C" will be interpreted or construed to prohibit Supplier from complying with any valid court order made under the laws of Ontario or the laws of Canada applicable in Ontario (but for clarity, not an order made under the laws of any other jurisdiction), on written notice to the Partnership.

Protection of Personal Data

12. Any Personal Data held by Supplier for the purpose of providing the IT Solution will be held in a secure physical and electronic environment in Ontario meeting or exceeding the standards relating to the protection of sensitive personal information set out in this Schedule.

13. Except with the prior written authorization of the Partnership, Supplier will not transfer or permit access to Personal Data to any person, including Authorized Personnel, or facility outside of Ontario.

14. To the extent that Supplier holds Personal Data, Supplier will not comingle Personal Data with any other data.

15. Supplier will maintain a record of access to the Partnership data, by Authorized Personnel or by any person from equipment controlled by Supplier, which record will include the identity of the person who accessed the Partnership data, the date and time of access and the duration of the session. Supplier will produce such record to the Partnership at its request and retain such record for a minimum of seven (7) years from the date on which the Agreement expires or terminates.

16. If the Partnership determines, in its sole discretion, that a practice or procedure used by Supplier to provide the IT Solution would violate a privacy requirement applicable to the Partnership, as a result of a legislative change, a finding, order or decision of a regulatory authority with jurisdiction over Personal Data, or for any other reason, the Partnership may amend this Agreement to vary or eliminate such practice or procedure on prior written notice to Supplier, subject to the Change Order Process in the Agreement.

17. Supplier will promptly advise the Partnership if it believes that any practice or procedure in which it is engaging in connection with the IT Solution contravenes a privacy requirement, or if it receives or learns of any complaint or allegation to that effect.

18. Supplier will use safeguards and meet a standard of protection that are appropriate for protecting sensitive information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal.

19. Without limiting the generality of section 8(c) above, Supplier will:

(a) ensure that Authorized Personnel receive sufficient training to be able to comply with the applicable Supplier Privacy Requirements;

(b) take reasonable steps, through means such as training, confidentiality agreements and the application of appropriate sanctions, to ensure Authorized Personnel comply with applicable Supplier Privacy Requirements;

(c) ensure that immediately upon termination or expiry of their employment by or affiliation with Supplier, access of Authorized Personnel to Personal Data is terminated and any and all Personal Data being held by Authorized Personnel is left with Supplier;

(d) terminate access of Authorized Personnel to Personal Data and replace Authorized Personnel where the acts or omissions of Authorized Personnel are reasonably likely to threaten the security and/or integrity of Personal Data or Supplier's compliance with the Supplier Privacy Requirements, and on the reasonable request of the Partnership; and

(e) not permit staff of any permitted subcontractor access to Personal Data unless and until such subcontractor has signed a written agreement requiring it to comply with applicable Supplier Privacy Requirements, including agreeing to the inspection and audit described in Section 23 of this Schedule "C" and permitting Supplier to terminate its agreement with such subcontractor where its acts or omissions are reasonably likely to threaten Supplier's compliance with the Supplier Privacy Requirements.

20. Supplier will co-operate with the Partnership, acting reasonably, where the Partnership requires Supplier's assistance in regard to:

(a) security or privacy events, including without limitation any breach, that could reasonably threat or threatens the security and/or integrity of Personal Data;

(b) inquiries, complaints, or investigations relating to Personal Data;

(c) assessments being conducted by or on behalf of the Partnership, including privacy impact and threat risk assessments, that involve the IT Solution.

21. Supplier will notify the Partnership:

(a) promptly, of any inquiries, complaints or investigations referred to in section 20(b) above;

(b) promptly, if it determines that, for any reason, it does not or will not be able to comply with this Schedule "C", outlining the particulars and the steps Supplier proposed to take to address the non-compliance or prevent the anticipated non-compliance; and

(c) notwithstanding paragraph (b) above, immediately upon becoming aware of the theft, loss, or unauthorized access, use, modification, disclosure or destruction of Personal Data or where there is a reasonable likelihood that such an event could have occurred.

22. Notwithstanding anything to the contrary in the Agreement, the Partnership may:

(a) make application for a court order preventing or terminating any non-compliance by Supplier with this Schedule "C"; and

(b) terminate the Agreement on notice in the event that the Partnership determines that Supplier has breached this Schedule "C", and Supplier has failed to cure the breach in accordance with Section 9.2 of the Agreement.

Audit, Inspection

23. In addition to the audit described in the Agreement, the Partnership or an independent auditor retained by the Partnership for the purpose that has entered into a mutually acceptable confidentiality agreement with the parties, will have the right, during normal business hours and upon reasonable notice to Supplier, to visit and inspect all locations at which Supplier, or any of its permitted subcontractors, accesses, uses, holds or stores Personal Data, to examine all equipment used, and all records in connection therewith, to make copies of such records and to ask questions of Authorized Personnel (including permitted subcontractors) reasonably required to verify Supplier's compliance with this Schedule "C" and otherwise to audit and verify, both physically and electronically, compliance by Supplier with this Schedule "C". Notwithstanding the preceding, the Partnership will have no duty to make any such visit, inspection, examination, audit or verification and will not incur any liability or obligation by reason of doing or not doing so.

Termination and Survival

24. Notwithstanding [section 8.6] of the Agreement, in the event of the termination or expiry of this Agreement, or at any other time at the Partnership's request in respect of some or all Personal Data, Supplier will forthwith at the Partnership's discretion, securely return to the Partnership or securely destroy all Personal Information held by Supplier pursuant to this Agreement without retaining any copies, excluding archival or long term back up storage that is not exclusive to Personal Data. Upon request, an officer's certificate attesting that such actions have been completed and that there are no tangible and/or available electronic versions of Personal Data being held by Supplier will be provided to the Partnership by Supplier, except for archival or long term back up storage that is not exclusive to Personal Data. Supplier undertakes not to recreate,

in whole or in part, any copy of Personal Data (including, but not limited to an electronic copy) at any time after the return or destruction of Personal Data. Where commercially reasonable to do so or as otherwise provided for in this Agreement, Supplier will apply procedures to segregate the Partnership data from other data sources. Supplier shall share its data destruction policy with the Partnership in relation to data that may be co-mingled with the Partnership data.

25. Notwithstanding the termination of the Agreement, to the extent that Supplier continues to have access to Personal Data for any reason, Supplier will continue to govern itself in accordance with the terms of this Schedule "C".

26. The obligations of Supplier under this Schedule "C", regarding ownership and control of Personal Information, access, use and non-disclosure of Personal Data and Authorized Personnel's compliance with such provisions, will survive the termination of the Agreement.

Schedule "D": Proposed Letter of Agreement - Term Sheet (LOA-TS)

SECURITY PROVISIONS

1. **Security.** The Parties acknowledge the fundamental importance of establishing logical and physical controls in order to maintain the security, integrity and availability of the IT Solution, and limit unauthorized access, destruction, loss or alteration to, and disclosure of, the Partnership's Confidential Information and any Personal Information, in all formats including but not limited to electronic and paper formats in accordance with this Agreement. As such, Supplier agrees to establish and maintain and to ensure each of its subcontractors establish and maintain minimum safeguards as defined below:

   (a) **Information Security Policy and Procedures.** Establish and maintain formal information security policies and procedures establishing controls around the Partnership's Confidential Information and Personal Information, and the systems that process them, in accordance with the requirements of the Partnership.

   (b) **Information Security Organization.** Define responsibility for the ongoing review of information security safeguards to reasonably ensure its continuing suitability, adequacy and effectiveness, in accordance with the requirements of the Partnership, and changing threats to security.

   (c) **Asset Management.** Define the inventory of data centre, facilities and systems that create, store, process and disseminate the Partnership's Confidential Information and Personal Information, and establish ownership and responsibility for the successful operation of security controls for each of those environments.

   (d) **Human Resources.** Establish and maintain controls to ensure that employees, contractors and third party staff are suitably screened and educated on security practices prior to being given access to the Partnership's data and the systems that process that data, and that all individual access to the Partnership's Confidential Information and Personal Information, is promptly removed upon termination of employment, agreement or contract with Supplier, or adjusted upon a change in role. At the request of the Partnership, Supplier will be obligated to provide a list of individuals that have access to IT resources related to the Partnership.

   (e) **Physical and Environmental Security.** Establish a security perimeter around the physical work environment and sensitive data processing facilities, and establish physical entry controls to reasonably ensure that only authorized individuals gain access to the environment, and environmental controls to protect against damage from fire, flood, and other forms of man-made or natural disasters.

   (f) **Communications and Operations Management.** Establish operating procedures and controls for the secure operations of systems and networks facilitating the access to the Partnership's Confidential Information and Personal Information in order to reasonably prevent accidental or deliberate misuse. Such controls include, but are not limited to, change management, least privileges granted, segregation of duties, separation of production environment from development/test environments, backups, network security, and the encryption of media in transit between the Partnership and Supplier. In addition, Supplier will maintain a secure communication

link (e-mail, telephony, etc.) to ensure that Confidential Information and Personal Information travelling between the two parties remains secure.

(g) **Access Controls.** Establish controls and procedures for the authorization, regular review and revocation of access at all levels of the system environment including physical access, network access, operating systems, applications and database access. Maintain suitable authentication controls to reasonably ensure that an individual's access rights to the Partnership's Confidential Information and Personal Information is appropriate for the individual's role regardless of how that individual is attempting to access that information or the location from which access is being attempted.

(h) **Information Systems Acquisition, Development and Maintenance.** Maintain an application development and maintenance framework that protects the integrity of the production application and associated source code from unauthorized and untested modifications. Such a framework shall establish control over the Partnership's Confidential Information and Personal Information, across all environments within the development lifecycle of systems.

(i) **Incident Management.** Establish policies and procedures for the timely communication and investigation of suspected breaches in the security of the Partnership's Confidential Information and Personal Information. At a minimum, communication of such incidents to the Partnership must take place prior to any discussion with regulators, clients, outside law enforcement agencies or representatives of the media. Incident investigations and associated information handling shall be performed in accordance with Applicable Law.

(j) **Business Continuity Management.** Establish appropriate policies and procedures to ensure continued provision of Services in accordance with timelines defined by the Parties as part of the Transition Services.

(k) **Compliance.** Establish policies and procedures to ensure that the design, operation and management of systems controlled by Supplier or its Subcontractors and processing the Partnership's Confidential Information and Personal Information meets the requirements of Applicable Law, and the requirements established in this Agreement.

(l) **Data Destruction and Disposal.** Supplier will implement processes and controls to ensure that any storage media or data is disposed or destroyed securely in accordance to the requirement of the Partnership.

(m) **Auditing.** Supplier will maintain wherever possible an audit trail of the associated activities by staff or automated processes. Supplier will make available upon the Partnership's request any reports related to specific actions.

(n) **Review.** Supplier shall conduct regular control reviews of security of the Services, including, as applicable, penetration testing and intrusion detection, malware alerts, and share the results of such reviews with the Partnership.

2. **Verification and Audit of Security Compliance.** Supplier represents and warrants that it maintains adequate internal audit functions to assess internal controls in its environment, and to protect the security and confidentiality of any of the Partnership's Confidential Information

and Personal Information which will be confirmed by the audit report referred to in the herein. Supplier agrees to provide documentation regarding its internal controls to the Partnership upon request. Upon the Partnership's request, Supplier will provide at the Partnership's expense a report of an independent, reputable, audit firm, which report shall be compliant with the Canadian Standard on Assurance Engagements (CSAE) 3416 Reporting on Controls at a Service Organization, as such standard may be superseded, amended or replaced from time-to-time. Each report shall cover the Services and the IT Solution for a consecutive twelve (12) month period ending March 31 in each year during the term of this Agreement. Supplier shall provide the Partnership with a copy of each report within thirty (30) Business Days following its receipt.

End of RFP