



REQUEST FOR PROPOSAL

RETURN BIDS TO:

Bids must be submitted by email and must be submitted ONLY to the following email address:

soumission.bid@aadnc-aandc.gc.ca

soumissionbid@sac-isc.gc.ca

REQUEST FOR PROPOSALS

Proposal to DIAND:

We hereby offer to sell to Her Majesty the Queen in right of Canada, as represented by the Minister of Indigenous and Northern Affairs Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the services listed herein and on any attached sheets at the price(s) set out therefor.

Title Electronic Dental Records System for ISC	
Solicitation Number 1000244928	
Date (YYYYMMDD) 2023-01-16	
Solicitation Closes At 9:00 AM	Time Zone Eastern Standard Time (EST)
On (YYYYMMDD) 2023-02-10	
Contracting Authority	
Name Miriam Britel	
Telephone Number (873) 355-2463	
Facsimile Number	
Email Address miriam.britel@sac-isc.gc.ca	
Destination(s) of Services ISC - FNIHB - Atlantic	
Security THIS REQUEST INCLUDES SECURITY PROVISIONS	
Instructions: See Herein	
Delivery Required See Herein	
Person Authorized to sign on behalf of Bidder	
Name	
Title	

Bidder
Name
Address
Telephone Number
GST/HST Number
QST Number



TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION 4

1.1 INTRODUCTION.....4

1.2 SUMMARY4

1.3 DEBRIEFINGS4

PART 2 - BIDDER INSTRUCTIONS 5

2.1 STANDARD INSTRUCTIONS, CLAUSES AND CONDITIONS.....5

2.2 SUBMISSION OF BIDS.....5

2.3 FORMER PUBLIC SERVANT.....5

2.4 ENQUIRIES - BID SOLICITATION.....6

2.5 APPLICABLE LAWS.....7

2.6 IMPROVEMENT OF REQUIREMENT DURING SOLICITATION PERIOD7

2.7 BID CHALLENGE AND RECOURSE MECHANISMS7

PART 3 - BID PREPARATION INSTRUCTIONS..... 8

3.1 BID PREPARATION INSTRUCTIONS8

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION 10

4.1 EVALUATION PROCEDURES.....10

4.2 BASIS OF SELECTION.....26

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION 28

5.1 CERTIFICATIONS REQUIRED WITH THE BID28

5.2 CERTIFICATIONS PRECEDENT TO CONTRACT AWARD AND ADDITIONAL INFORMATION28

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS..... 29

6.1 SECURITY REQUIREMENTS29

PART 7 - RESULTING CONTRACT CLAUSES 30

7.1 STATEMENT OF WORK.....30

7.2 STANDARD CLAUSES AND CONDITIONS.....30

7.3 SECURITY REQUIREMENTS30

7.4 TERM OF CONTRACT31

7.5 AUTHORITIES32

7.6 PROACTIVE DISCLOSURE OF CONTRACTS WITH FORMER PUBLIC SERVANTS33

7.7 PAYMENT34

7.8 INVOICING INSTRUCTIONS35

7.9 CERTIFICATIONS AND ADDITIONAL INFORMATION.....35

7.10 APPLICABLE LAWS.....35

7.11 PRIORITY OF DOCUMENTS35

7.12 INSURANCE36

7.13 LIMITATION OF LIABILITY36

7.14 DISPUTE RESOLUTION.....37

ANNEX “A” 43

STATEMENT OF WORK43

ANNEX “B” 57

BASIS OF PAYMENT57



ANNEX “C” 59
SECURITY REQUIREMENTS CHECK LIST59

ANNEX “D” 67
DEFINITIONS.....67



PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

- Part 1 General Information: provides a general description of the requirement;
- Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;
- Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;
- Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;
- Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;
- Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and
- Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Work, the Basis of Payment, the Security Requirements Checklist, and any other annexes.

1.2 Summary

- 1.2.1 Indigenous Services Canada (ISC) has a requirement for the implementation of an Electronic Dental Records system for the collection, management, storage, and sharing of dental patient data and information for the Atlantic Region.

It is intended to result in the award of one contract for the delivery of the services and the term for the provision of the services will be from Contract award to March 31, 2027 and four (4) option periods.

- 1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the [Contract Security Program](http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) of Public Works and Government Services Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html>) website.

- 1.2.3 The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), the Canada-United Kingdom Trade Continuity Agreement, Canada-Ukraine Free Trade Agreement, Canada-Peru Free Trade Agreement, Canada-Panama Free Trade Agreement, Canada-Korea Free Trade Agreement, Canada-Honduras Free Trade Agreement, Canada-Colombia Free Trade Agreement, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Canada-Chile Free Trade Agreement and the Canadian Free Trade Agreement (CFTA).

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.



PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the [Standard Acquisition Clauses and Conditions Manual](https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The [2003](#) (2022-03-29) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of [2003](#), Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days

Insert: 180 days

2.2 Submission of Bids

Bids must be submitted only to Indigenous Services Canada (ISC) by the date, time and place indicated on page 1 of the bid solicitation.

Due to the nature of the bid solicitation, bids transmitted by any other means to ISC will not be accepted.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause, "former public servant" is any former member of a department as defined in the [Financial Administration Act](#), R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

- a. an individual;
- b. an individual who has incorporated;
- c. a partnership made of former public servants; or
- d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the



implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the [Public Service Superannuation Act](#) (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the [Supplementary Retirement Benefits Act](#), R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the [Canadian Forces Superannuation Act](#), R.S., 1985, c. C-17, the [Defence Services Pension Continuation Act](#), 1970, c. D-3, the [Royal Canadian Mounted Police Pension Continuation Act](#), 1970, c. R-10, and the [Royal Canadian Mounted Police Superannuation Act](#), R.S., 1985, c. R-11, the [Members of Parliament Retiring Allowances Act](#), R.S. 1985, c. M-5, and that portion of pension payable to the [Canada Pension Plan Act](#), R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes () No ()**

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

- a. name of former public servant;
- b. date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with [Contracting Policy Notice: 2019-01](#) and the [Guidelines on the Proactive Disclosure of Contracts](#).

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes () No ()**

If so, the Bidder must provide the following information:

- a. name of former public servant;
- b. conditions of the lump sum payment incentive;
- c. date of termination of employment;
- d. amount of lump sum payment;
- e. rate of pay on which lump sum payment is based;
- f. period of lump sum payment including start date, end date and number of weeks;
- g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than five (5) calendar days before the bid closing date. Enquiries received after that time may not be answered.



Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Nova Scotia, New Brunswick, Newfoundland & Labrador and Prince Edward Island.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.6 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least ten (10) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Bid Challenge and Recourse Mechanisms

- (a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.
- (b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's [Buy and Sell](#) website, under the heading "[Bid Challenge and Recourse Mechanisms](#)" contains information on potential complaint bodies such as:
 - Office of the Procurement Ombudsman (OPO)
 - Canadian International Trade Tribunal (CITT)
- (c) Suppliers should note that there are **strict deadlines** for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.



PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Canada requests that the Bidder submits its bid electronically in accordance with section 8 of the 2003 standard instructions and as amended in Part 2 - Bidder Instructions, Article 2.1 Standard Instructions, Clauses and Conditions. Bidders are required to provide their bid in a single transmission. The total size of the email, including all attachments, **must not exceed 10 megabytes (MB)**. It is solely the Bidder's responsibility to ensure that the total size of the email does not exceed this limit.

The bid must be gathered per section and separated as follows:

Section I: Technical Bid

Section II: Financial Bid

Section III: Certifications

Section IV: Additional Information

Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Section II: Financial Bid

3.1.1 Bidders must submit their financial bid in accordance with Pricing Schedule detailed in the Basis of Payment in Annex "B".

3.1.2 Electronic Payment of Invoices – Bid

Bidders will accept Direct Deposit (Domestic and International) for payment of invoices.

The Bidder is not obligated to accept payment by Electronic Payment Instruments.

Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

3.1.3 Exchange Rate Fluctuation

[C3011T](#) (2013-1-06), Exchange Rate Fluctuation

3.1.4 SACC Manual Clauses

Section III: Certifications

Bidders must submit the certifications and additional information required under Part 5.

Section IV: Additional Information

3.1.5 Bidder's Proposed Sites or Premises Requiring Safeguarding Measures

3.1.5.1 As indicated in Part 6 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals' sites or premises for which safeguarding measures are required for Work Performance:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State



Postal Code / Zip Code
Country

- 3.1.5.2** The Company Security Officer must ensure through the Contract Security Program that the Bidder and proposed individuals hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.



PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

- (a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.
- (b) An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

4.1.1 Technical Evaluation

4.1.1.1 Mandatory Technical Criteria

The bid must meet the mandatory technical criteria specified below. The Bidder must provide the necessary documentation to support compliance with this requirement.

Bids which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

Mandatory Technical Criteria (MT) –			
For the purpose of the mandatory technical criteria specified below, the experience of the Bidder and its possible subcontractors, affiliates and suppliers will be considered.			
Number	Mandatory Technical Criterion	Cross Reference to proposal	Met Y/N
MT1	The proposed Electronic Dental Records System (EDR) must be modifiable and configurable to meet needs of organization.		
MT2	The proposed Electronic Dental Records System (EDR) must be deployable using Cloud technology able to be accredited to Government of Canada Protected B Security Profile.		
MT3	The proposed Electronic Dental Records System (EDR) must interface/link with current and new digital radiography systems.		
MT4	The proposed Electronic Dental Records System (EDR) must provide remote, point-of-care access to dental records.		
MT5	The proposed Electronic Dental Records System (EDR) have different levels of approved access to EDR system.		
MT6	The proposed Electronic Dental Records System (EDR) must have the ability to print hard copies of dental records.		
MT7	System must have the ability to run reports for service		



	and program evaluation.		
MT8	The proposed Electronic Dental Records System (EDR) must have the ability to upload digitized copies of paper-based dental records and existing digital x-ray files into EDR system as required.		
MT9	The proposed Electronic Dental Records System (EDR) must have the ability to upload scanned letters from external providers (e.g., dental specialists, physicians).		
MT10	Bidder must provide support during business hours Monday to Friday, from 8:00 am to 5:00 pm Atlantic Standard Time.		
MT11	Bidder must provide published Service Level Agreement for the proposed system. The included service level commitments must provide ISC with warranty, maintenance and support services. Support services must be provided in the language of user's choice of either English or French and may be delivered by telephone, e-mail, mobile messaging or web-based tools, as requested. The agreement must be signed and becomes binding prior to system launch.		
MT12	The proposed Electronic Dental Records System (EDR) must include the capability for users to report and track issues, either online or through telephone support.		
MT13	Processing and storage capabilities of the system must have the ability to adapt and support increasing amount of data and increasing number of users.		
MT14	The proposed Electronic Dental Records System (EDR) must support a minimum of 25 active/concurrent users.		
MT15	The proposed Electronic Dental Records System (EDR) must support creation and management of at least 25,000 records per year.		
MT16	The proposed Electronic Dental Records System (EDR) must upload at least .pdf, .doc, .docx, .jpg files, x-rays to support the dental office operation.		
MT17	The proposed Electronic Dental Records System (EDR) must allow for file size up to 10 megabytes without warning and attachments of size larger than 10 megabytes must trigger a warning to the user.		
MT18	The proposed Electronic Dental Records System		



	(EDR) must have encrypted Cloud-based data storage.		
MT19	The proposed Electronic Dental Records System (EDR) must allow uploading of colored intra-oral and facial photos or any other relevant information required for patient files.		
MT20	The proposed Electronic Dental Records System (EDR) must comply or can be modified to comply with Official Languages Act by being functionally equivalent in English and French and must allow users to work in the Canadian official language of their choice. Official Languages Act is here: Official Languages Act		
MT21	The proposed Electronic Dental Records System (EDR) must comply with Government of Canada standards on accessibility and usability. Must meet the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 .		
MT22	The proposed Electronic Dental Records System (EDR) must meet all of the Government of Canada policies on Service and Digital Standards: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603 .		
MT23	The proposed Electronic Dental Records System (EDR) must comply with Security Requirements for the secure handling, processing and storing of Protected B information.		
MT24	The proposed Electronic Dental Records System (EDR) must adhere to IM requirements (i.e., retention period and disposition).		
MT25	The proposed Electronic Dental Records System (EDR) Browser Configuration: <ul style="list-style-type: none"> a) for Internet based user interfaces, all user interfaces must be compatible with the standard ISC Internet browsers (Chrome, Edge, etc.) at the time the system is deployed to production and be kept current with subsequent versions when ISC upgrades to a new standard Internet browser, at no additional cost. b) for public facing Internet sites, all user interfaces must be compatible with the latest minus 2 versions of the approved ISC browsers, Chrome, Edge, and Safari. 		
MT26	The proposed Electronic Dental Records System (EDR) must incorporate input validation.		
MT27	The proposed Electronic Dental Records System		



	(EDR) must incorporate data validation.		
MT28	The proposed Electronic Dental Records System (EDR) must have the ability to remove duplicate data.		
MT29	The proposed Electronic Dental Records System (EDR) must incorporate Government of Canada-approved backup and restore functionality. The System must, on a daily basis, back up all ISC user credentials, data and files (e.g., audit records, documents, contact lists) onto a backup system, stored at a different location from the primary data center. Backups must also be stored within Canadian borders and encrypted.		
MT30	The proposed Electronic Dental Records System (EDR) must provide access controls.		
MT31	The proposed Electronic Dental Records System (EDR) must provide audit trail. Actions to be logged such as: <ul style="list-style-type: none"> • File creation • File deletion • Modifications • Logon/logoff information 		
MT32	The proposed Electronic Dental Records System (EDR) must interoperate with digital radiography system.		
MT33	The proposed Electronic Dental Records System (EDR) must be designed using current technologies, frameworks and coding languages that will continue to be supported by Bidder/User Community for the duration of EDR system's expected lifespan.		
MT34	The proposed Electronic Dental Records System (EDR) must respond to commands within 3 seconds under normal operating conditions.		
MT35	The proposed Electronic Dental Records System (EDR) must ensure that when a user performs a Logoff, or when a user is idle for a set period of time, the respective user session is terminated.		
MT36	The proposed Electronic Dental Records System (EDR) must restore data in the event of a failure (i.e., EDR system is capable of restoring all data saved prior to point of failure).		
MT37	The proposed Electronic Dental Records System (EDR) must have a recovery time of 24 hours in the		



	event of a failure (i.e., EDR system capable of recovering within 24 hours).		
MT38	Bidder must provide a Disaster Recovery Plan (DRP).		
MT39	The proposed Electronic Dental Records System (EDR) must be available 99% of the time, 7 days a week.		
MT40	The proposed Electronic Dental Records System (EDR) must meet all applicable ISC/CIRNAC security and privacy requirements. Must ensure adequate protection of data according to IT standards for Protected B information. In the SOW, see: ANNEX A – Tier 2 (Information categorized Up to and including Protected B) SECURITY REQUIREMENTS PRECEDENT TO CONTRACT AWARD FOR SOFTWARE AS A SERVICE CONTRACTS		
MT41	The proposed Electronic Dental Records System (EDR) must be able to provide required evidence to successfully meet Protected B accreditation		
MT42	The proposed Electronic Dental Records System (EDR) must have ability to upload digitized copies of paper-based dental records.		
MT43	The proposed Electronic Dental Records System (EDR) must have ability to upload existing digital x-ray files as required and sync with appropriate patient records.		
MT44	The Bidder is required to provide READ Access and privileges to the ISC DBA team, in order to perform the required data extraction or duplication from the Bidder-system database into the departmental infrastructure premises.		
MT45	The proposed Electronic Dental Records System (EDR) must allow users with Administrator permissions to add/modify/delete Electronic Dental Records (EDRs). Must offer ISC Administrators and Coordinators the capability to manage user access control (including privacy) and permission settings.		
MT46	Privacy settings of the system must have the ability to restrict viewing permissions of employee data based on organizational structure.		
MT47	The proposed Electronic Dental Records System (EDR) must be able to record users' name, role and responsibilities to maintain accurate historical audit		



	trail.		
MT48	The proposed Electronic Dental Records System (EDR) must be able to record all accesses to client data.		
MT49	The proposed Electronic Dental Records System (EDR) must support two factor authentication.		
MT50	The proposed Electronic Dental Records System (EDR) must allow modification of X-Number to Status Number (SN) in a client's record if client receives SN after their initial visit. Bidder must allow the addition/modification of SNs to a record by Administrators only. [SN is derived from the Status Verification System (SVS). The function of the SVS system is to provide Status Numbers to Clients regarding their eligibility to use the services provided.]		
MT51	The proposed Electronic Dental Records System (EDR) must allow access to approved external users (i.e., non-Internal/non-GoC users).		
MT52	The proposed Electronic Dental Records System (EDR) must allow configuration of the roles as outlined in Table 1.1 Authorized Users and Roles of the SOW.		
MT53	The proposed Electronic Dental Records System (EDR) must not allow deletion or modification of digitally signed entries or records.		
MT54	The proposed Electronic Dental Records System (EDR) must allow saving and signing.		
MT55	The proposed Electronic Dental Records System (EDR) must have the ability to auto save.		
MT56	The proposed Electronic Dental Records System (EDR) must ask the user to verify signature.		
MT57	The proposed Electronic Dental Records System (EDR) must provide a reminder if user leaves an entry/record digitally unsigned.		
MT58	The proposed Electronic Dental Records System (EDR) must store metadata with the Electronic Data Record.		
MT59	The proposed Electronic Dental Records System (EDR) must allow disposition rules for records management.		
MT60	The proposed Electronic Dental Records System (EDR) must allow searching of data records by last		



	name, first name, gender, date of birth or Status Number/X-Number.		
MT61	The proposed Electronic Dental Records System (EDR) must allow for remote, point of care access to electronic dental records.		
MT62	The proposed Electronic Dental Records System (EDR) must be a cloud-based, Software as a Service (SaaS) solution that can manage Protected B information.		
MT63	The proposed Electronic Dental Records System (EDR) must be deployable across four Atlantic provinces.		
MT64	The proposed Electronic Dental Records System (EDR) must provide charts that cover a lifetime of activity.		
MT65	The proposed Electronic Dental Records System (EDR) must be able to upload digitized copies of paper consent forms, letters from specialists, etc. and link them to the appropriate client electronic dental record.		
MT66	The proposed Electronic Dental Records System (EDR) must store digital radiography files and link to appropriate client electronic dental record.		
MT67	The proposed Electronic Dental Records System (EDR) must have client odontogram as a feature.		
MT68	The proposed Electronic Dental Records System (EDR) must allow recording of treatment notes.		
MT69	The proposed Electronic Dental Records System (EDR) must display daily appointment schedule.		
MT70	The proposed Electronic Dental Records System (EDR) must allow entry of a unique identifier (eg. Status Number, X-Number) to each client electronic dental record.		
MT71	The proposed Electronic Dental Records System (EDR) must interface/link with current and new digital radiography systems.		
MT72	The proposed Electronic Dental Records System (EDR) must be able to connect to a printer and allow printing of required sections of EDRs.		
MT73	The proposed Electronic Dental Records System (EDR) must be able to connect to a scanner and allow scanning, as well as uploading of scanned material.		



MT74	The proposed Electronic Dental Records System (EDR) must have ability to generate reports for service evaluation.		
MT75	The proposed Electronic Dental Records System (EDR) must have ability to generate reports for program evaluation.		
MT76	The proposed Electronic Dental Records System (EDR) must be scalable to meet National growth.		

4.1.1.2 Point Rated Technical Criteria

Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below.

Bids which fail to obtain the required minimum number of points specified will be declared non-responsive. Each point rated technical criterion should be addressed separately.

Point Rated Technical Criteria (RT)	Required Minimum Number of Points	Maximum Available Points
RT1		10
RT2		10
RT3		10
RT4		5
RT5		5
RT6		10
RT7		10
RT8		10
RT9		5
RT10		10
RT11		15
RT12		15
RT13		15
RT14		15
RT15		15
RT16		15
RT17		15
RT18		15
RT19		15
RT20		20
Overall Score	135	240

	Rated Technical Requirements: Resource Experience (RTR)	Bid Preparation Instructions	Weighting (Points)
RT1.0	Bidder should demonstrate support services offered within Canada.		Points will be awarded on the following basis: 0 points International company without support services in Canada



			<p>5 points International company with support services in Canada</p> <p>10 points Canadian-based company</p> <p>Maximum Points: 10 points</p>
RT2.0	Bidder should have extensive experience implementing EDR software.	<p>To demonstrate its experience, the Bidder must provide at least the following information for each client reference for which the experience meets the requirements of evaluation criterion RT2:</p> <ol style="list-style-type: none"> 1) Short description of the services provided to the client; 2) The period of time over which the service was provided per month, in a format including month and year information, (e.g., from (month/year) to (month/year)); and 3) The name of the client for whom the services work was done as well as the name and current e-mail address or telephone number of the client. 	<p>Points will be awarded on the following basis:</p> <p>5 points Less than 10 years' experience implementing EDRS as of bid closing</p> <p>10 points More than 10 years' experience implementing EDRS as of bid closing</p> <p>Maximum Points: 10 points</p>
RT3.0	Bidder should have experience working with larger organizations (e.g., multi-clinic practices, corporations, federal, municipal, provincial, non-profit organizations).	<p>To demonstrate its experience, the Bidder must provide at least the following information for each client reference for which the experience meets the requirements of evaluation criterion RT3:</p> <ol style="list-style-type: none"> 1) Short description of the services provided to the client; 2) The period of time over which the service was provided per month, in a format including month and year information (e.g., from (month/year) to (month/year)); and 3) The name of the client for whom the services work was done as well as the name and current e-mail 	<p>Points will be awarded on the following basis:</p> <p>0 points No experience</p> <p>5 points Some experience working with larger organizations (5 years or less)</p> <p>10 points Significant experience working with larger organizations (greater than 5 years)</p> <p>Maximum Points: 10 points</p>



		address or telephone number of the client.	
RT4.0	Bidder should have scaled licensing fees (e.g., allow multiple users per license; not only allow per person licensing).		Points will be awarded on the following basis: 0 points No scaled licensing fees 5 points Scaled licensing fees available Maximum Points: 5 points
RT5.0	Bidder should have the ability to install software on-site.		Points will be awarded on the following basis: 0 points Unable to install software on-site 5 points Able to install software on-site Maximum Points: 5 points
RT6.0	Bidder should have a comprehensive training plan to ensure ease of use and learning of the system based on user needs.	In order to meet the requirements of evaluation criterion RT6, the Bidder must provide an example training plan.	Points will be awarded on the following basis: 0 points Bidder does not have a training plan 5 points Bidder has a standardized training plan for all users 10 points Bidder has a training plan customizable to user needs Maximum Points: 10 points



<p>RT7.0</p>	<p>Bidder should have the ability to offer training, in person and/or virtually.</p>	<p>To demonstrate its experience, the Bidder must provide at least the following information for each client reference for which the experience meets the requirements of evaluation criterion RT7:</p> <ol style="list-style-type: none"> 1) Short description of the type of training provided to the client; 2) The period of time over which the service was provided per month, in a format including month and year information (e.g., from (month/year) to (month/year)); and 3) The name of the client for whom the training was done as well as the name and current e-mail address or telephone number of the client. 	<p>Points to will be awarded on the following basis:</p> <p>0 points No documentation demonstrating the Bidder's experience offering training is provided</p> <p>5 points Documentation demonstrating the Bidder's experience offering training is provided, per the instructions described</p> <p>10 points Documentation demonstrating the Bidder's experience offering training is provided, per the instructions described, with additional points supporting the training experience</p> <p>Maximum Points: 10 points</p>
<p>RT8.0</p>	<p>Bidder should have ongoing support services for training, on an as needed basis.</p>		<p>Points to be awarded on the following basis:</p> <p>0 points Bidder does not offer ongoing training support services</p> <p>5 points Bidder offers ongoing training support services with limitations (e.g., fixed monthly frequency)</p> <p>10 points Bidder offers ongoing training support services, as needed</p> <p>Maximum Points: 10 points</p>
<p>RT9.0</p>	<p>The proposed Electronic Dental Records System (EDR) should have the ability to send email notifications to clients (e.g., appointment reminders two in advance).</p>		<p>Points to be awarded on the following basis:</p> <p>0 points System does not have ability to send email notifications to clients</p> <p>5 points System has ability to send email notifications to clients</p> <p>Maximum Points: 5 points</p>



RT10.0	The proposed Electronic Dental Records System (EDR) should be expandable for implementation across Canada.		<p>Points to be awarded on the following basis:</p> <p>0 points System not expandable for implementation across Canada</p> <p>5 points System expandable for implementation across Canada, with limitations (e.g., excludes remote areas)</p> <p>10 points System expandable for implementation across Canada, without limitations</p> <p>Maximum Points: 10 points</p>
RT11.0	<p>Pre-Implementation Plan</p> <p>The Bidder should provide a detailed Pre-Implementation Plan covering the Pre-Implementation Phase from the date of Contract Award to the Implementation Date to perform all activities defined in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT11, the Bidder must provide a pre-implementation plan which includes at least the following requirements:</p> <ul style="list-style-type: none"> • A detailed list of all tasks to be completed; • An explanation or rationale for including the tasks; • A Responsibility assignment matrix describing the participation required from the Bidder and the Project Authority in completing the tasks and deliverables for the pre-implementation; • Any dependencies where Canada's involvement is required; and • A schedule that illustrates the critical path and associated milestones. 	<p>Points will be awarded on the following basis:</p> <p>0 points No pre-implementation is plan provided</p> <p>5 points A pre-implementation plan is provided, but does not include all listed minimum requirements</p> <p>10 points A pre-implementation plan is provided, including all listed minimum requirements</p> <p>15 points A pre-implementation plan is provided, including all listed minimum requirements and additional details</p> <p>Maximum Points: 15 points</p>
RT12.0	<p>Operations Plan</p> <p>The Bidder should provide a detailed Operations Plan covering the Operations Phase of the contract as specified in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT12, the Bidder must provide an Operations plan which includes at least the following requirements:</p> <ul style="list-style-type: none"> • A detailed explanation of the Bidder's approach for the 	<p>Points will be awarded on the following basis:</p> <p>0 points No operations plan is provided</p> <p>5 points An incomplete operations plan is provided</p> <p>10 points A complete operations</p>



		<p>SOW;</p> <ul style="list-style-type: none"> • A schedule that illustrates the critical path and associated milestones; • Responsibility assignments; • The approach for meeting service delivery standards; • Any dependencies where Canada’s involvement is required; and • How the Bidder’s Quality Assurance (QA) processes and Information Technology (IT) solutions will be applied. 	<p>15 points</p> <p>plan is provided A complete operations plan with additional points supporting an operations plan is provided</p> <p>Maximum Points: 15 points</p>
<p>RT13.0</p>	<p>Business Continuity and Disaster Recovery</p> <p>The Bidder should describe its approach to Business Continuity and Disaster Recovery.</p>	<p>In order to meet the requirements of evaluation criterion RT13, the Bidder must provide a text explaining their business continuity and disaster recovery plan including their approach for electronic and paper based records.</p>	<p>Points will be awarded on the following basis:</p> <p>0 points No business continuity and disaster recovery plan is provided</p> <p>5 points A non-comprehensive business continuity and disaster recovery plan is provided</p> <p>10 points A comprehensive business continuity and disaster recovery plan is provided</p> <p>15 points A comprehensive business continuity and disaster recovery plan, with additional points supporting a business continuity and disaster recovery plan is provided</p> <p>Maximum Points: 15 points</p>
<p>RT14.0</p>	<p>Risk Management</p> <p>The Bidder should provide a risk management plan for each contract phase to successfully complete all requirements specified in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT14, the Bidder must provide a risk management plan which includes a methodology for at least the following points:</p> <ul style="list-style-type: none"> • Identification of all major risks; • An analysis of the risk by 	<p>Points will be awarded on the following basis:</p> <p>0 points No risk management plan is provided</p> <p>5 points An incomplete risk management plan is provided</p> <p>10 points A complete risk management plan is provided</p> <p>15 points A complete risk</p>



		<p>probability and impact;</p> <ul style="list-style-type: none"> • Identification of appropriate mitigation or avoidance strategies; and • On-going risk management procedures and practices. 	<p>management plan with additional points supporting a risk management plan is provided</p> <p>Maximum Points: 15 points</p>
RT15.0	<p>Requirements Compliance</p> <p>The Bidder should describe their proposed approach in detail on how it will meet the requirements compliance when implementing an information system to facilitate the delivery of services as described in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT16, the Bidder must provide a requirements compliance plan which includes at least the following requirements:</p> <ul style="list-style-type: none"> • All functionalities and reporting capabilities of the proposed solution; • Physical infrastructure and facilities; • System performance specifications; • Data conversion and migration; and • Security. 	<p>Points will be awarded on the following basis:</p> <p>0 points No requirements compliance plan is provided</p> <p>5 points An incomplete requirements compliance plan is provided</p> <p>10 points A complete requirements compliance plan is provided</p> <p>15 points A complete requirements compliance plan with additional points supporting a requirements compliance plan is provided</p> <p>Maximum Points: 15 points</p>
RT16.0	<p>Solution Architecture</p> <p>The Bidder should provide a detailed description of their solution architecture of the proposed information system to facilitate the delivery of services as described in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT17, the Bidder must provide a text of a description of their solution architecture which includes at least the following points:</p> <ul style="list-style-type: none"> • Detailed Solution Architecture including the business view, information view, application/component view, technology view and deployment view; • The maintainability of the solution. This quality attribute relates the level of effort required to identify a problem and correct it; 	<p>Points will be awarded on the following basis:</p> <p>0 points No description of the solution architecture is provided</p> <p>5 points An incomplete description of the solution architecture is provided</p> <p>10 points A complete description of the solution architecture is provided</p> <p>15 points A complete description of the solution architecture with additional points describing the solution architecture is provided</p>



		<ul style="list-style-type: none"> • The extensibility of the solution. This quality attribute relates the ability to extend a system and the level of effort required to implement the extension. The following areas will be considered: workflows, data elements, user interfaces, business rules, data validation and parametrization; • The solution's level of fault tolerance; and • The solution's level of scalability. 	Maximum Points: 15 points
RT17.0	<p>Solution Life-Cycle Management</p> <p>The Bidder should provide a detailed description of their management of the solution life-cycle of the proposed information system to facilitate the delivery of services as described in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT18, the Bidder must provide a text of a description of their management of the solution life-cycle which includes at least the following points:</p> <ul style="list-style-type: none"> • Methodology and tools used; • Implementation plan and Software Development Life Cycle (SDLC); • Requirement management; • Testing and Quality Assurance; • Release management; and • Defect management. 	<p>Points will be awarded on the following basis:</p> <p>0 points No description of the management of the solution life-cycle is provided</p> <p>5 points An incomplete description of the management of the solution life-cycle is provided</p> <p>10 points A complete description of the management of the solution life-cycle is provided</p> <p>15 points A complete description of the management of the solution life-cycle with additional points describing the management of the solution life-cycle is provided</p> <p>Maximum Points: 15 points</p>
RT18.0	<p>Technical Operations</p> <p>The Bidder should provide a detailed description of their technical operations of the proposed information system to facilitate the delivery of services as described in the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT19, the Bidder must provide a text of a description of the system's technical operations which includes at least the following points:</p> <ul style="list-style-type: none"> • System operations and maintenance; and 	<p>Points will be awarded on the following basis:</p> <p>0 points No description of the technical operations of the system is provided</p> <p>5 points An incomplete description of the technical operations of the system is provided</p> <p>10 points A complete description</p>



		<ul style="list-style-type: none"> System health monitoring including escalation processes. 	<p>15 points</p> <p>of the technical operations of the system is provided A complete description of the technical operations of the system with additional points describing the technical operations of the system is provided</p> <p>Maximum Points: 15 points</p>
RT19.0	<p>Reporting & Business Intelligence Capabilities</p> <p>The Bidder should provide an approach to implementing reporting solutions in order to meet all reporting and business intelligence requirements specified in the SOW.</p>	<p>To demonstrate its experience, the Bidder must provide at least the following information for each client reference for which the experience meets the requirements of evaluation criterion RT20:</p> <ol style="list-style-type: none"> Short description of the proposed approach and the requirements will be met; Assessment of the complexity of the work; and Identification of risk factors and mitigation strategies. 	<p>Points will be awarded on the following basis:</p> <p>0 points No plan for implementing reporting solutions is provided</p> <p>5 points An incomplete plan for implementing reporting solutions is provided</p> <p>10 points A complete plan for implementing reporting solutions is provided</p> <p>15 points A complete plan for implementing reporting solutions with additional points supporting the plan for implementing reporting solutions is provided</p> <p>Maximum Points: 15 points</p>
RT20.0	<p>Quality Assurance (QA)</p> <p>The Bidder should provide details on its quality assurance processes and related quality management systems including descriptions of all policies, processes, controls and procedures required to complete the requirements of the SOW.</p>	<p>In order to meet the requirements of evaluation criterion RT21, the Bidder must provide a text which includes at least the following points:</p> <ul style="list-style-type: none"> The set of procedures that cover all key processes; Identification of organization roles and responsibilities for QA; The related monitoring processes and controls to ensure they are effective; 	<p>Points will be awarded on the following basis:</p> <p>0 points No quality assurance processes and procedures are evident</p> <p>5 points Bidder has a quality assurance process and quality management system but there are major inconsistencies between the various aspects of its quality</p>



		<ul style="list-style-type: none"> • QA record keeping practices; • Verification processes to ensure consistent service delivery; and • Processes that ensure continual improvements and lessons learned. 	<p>10 points assurance and quality management systems Bidder has an effective quality assurance process and quality management system but there are minor inconsistencies between the various aspects of its quality assurance and quality management systems</p> <p>15 points Bidder has a highly effective quality assurance process and quality management system</p> <p>20 points Bidder has a highly effective quality assurance process and quality management system supported by a third party (such as ISO or ISO equivalent) certification</p> <p>Maximum Points: 20 points</p>
--	--	--	--

4.1.2 Financial Evaluation

4.1.2.1 Mandatory Financial Criteria

SACC Manual Clause [A0220T](#) (2014-06-26), Evaluation of Price-Bid

4.2 Basis of Selection

4.2.1 Highest Combined Rating of Technical Merit and Price

1. To be declared responsive, a bid must:
 - a. comply with all the requirements of the bid solicitation; and
 - b. meet all mandatory criteria; and
 - c. obtain the required minimum of 135 points overall for the technical evaluation criteria which are subject to point rating. The rating is performed on a scale of 240 points.
2. Bids not meeting (a) or (b) or (c) will be declared non-responsive.
3. The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70 % for the technical merit and 30 % for the price.
4. To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70 %.



5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30 %.
6. For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.
7. Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively. The total available points equals 135 and the lowest evaluated price is \$45,000 (45).

Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)				
		Bidder 1	Bidder 2	Bidder 3
Overall Technical Score		115/135	89/135	92/135
Bid Evaluated Price		\$55,000.00	\$50,000.00	\$45,000.00
Calculations	Technical Merit Score	$115/135 \times 70 = 59.6$	$89/135 \times 70 = 46.1$	$92/135 \times 70 = 47.0$
	Pricing Score	$45/55 \times 30 = 24.5$	$45/50 \times 30 = 27.0$	$45/45 \times 30 = 30.0$
Combined Rating		84.1	73.1	77.0
Overall Rating		1st	3rd	2nd



PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the [Forms for the Integrity Regime](http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html) website (<http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html>), to be given further consideration in the procurement process.

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the [Ineligibility and Suspension Policy](http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html>), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Federal Contractors Program for Employment Equity - Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the page of the [Employment and Social Development Canada \(ESDC\) - Labour's](https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#) website (<https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#>).

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid list at the time of contract award.



PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

1. Before award of a contract, the following conditions must be met:
 - (a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;
 - (b) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
 - (c) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;
 - (d) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
 - (e) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.
2. Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.
3. For additional information on security requirements, Bidders should refer to the [Contract Security Program](http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) of Public Works and Government Services Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html>) website.



PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex "A".

7.2 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the [Standard Acquisition Clauses and Conditions Manual](https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.

7.2.1 General Conditions

[2035](#) (2022-12-01), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

7.2.2 Supplemental General Conditions

[4002](#) (2010-08-16), Supplemental General Conditions – Software Development or Modification Services, apply to and form part of the Contract;

[4003](#) (2010-08-16), Supplemental General Conditions – Licensed Software, apply to and form part of the Contract;

[4004](#) (2013-04-25), Supplemental General Conditions – Maintenance and Support Services for Licensed Software, apply to and form part of the Contract; and

[4006](#) (2010-08-16), Supplemental General Conditions – Contractor to Own Intellectual Property Rights in Foreground Information, apply to and form part of the Contract.

7.3 Security Requirements

7.3.1 The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Contract.

1. Pursuant to the Policy on Government Security, the nature of the services to be provided under this contract requires a valid Government of Canada (GoC) personnel Security Screening at the level of **Reliability Status** for the Contractor, authorized resources and any sub-contractors to be assigned to conduct the work.
2. Prior to the commencement of the work, the Contractor and each authorized resources involved in the performance of the work under this contract must each hold a valid Security Screening at the level of **Reliability Status** during the lifetime of the contract.
3. The Contractor and its personnel requiring access to PROTECTED information, assets or sensitive work site(s) must EACH hold a valid Security Screening at the level of **Reliability Status**.
4. The Contractor MUST NOT possess or safeguard **PROTECTED** information/assets at their organization's premises until written permission from the security in contracting team of Indigenous Services Canada (ISC). After permission has been granted, these tasks may be performed up to the level of **Protected B**.
5. The Contractor MUST NOT remove any **Sensitive** information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restrictions.
6. The Contractor MUST NOT utilize its Information Technology (IT) systems to electronically process, produce or store any sensitive information until written permission from the security in contracting



team of ISC. After permission has been granted, these tasks may be performed up to the level of **Protected B**

7. Subcontracts are not to be awarded without the prior written permission from the security in contracting team of ISC.
8. Any substitute or alternate resource proposed for this contract:
 - a) must be approved by the Security and Emergency Services Divisions of Indigenous Services Canada; and,
 - b) must hold a valid GoC Security Screening at the level of **Reliability Status**, before gaining access to designated information or assets.
9. Under this contract, if a Contractor submits a resource who is subsequently found to not meet the Security requirements, the Department may immediately terminate the contract with no obligation to replace the resource with a resource from the same Contractor or to pay any invoice for work undertaken by this resource.
10. This contract only has force or effect for as long as the Security Screening at the level of **Reliability Status** is valid. During the lifetime of this contract, if the Security Screening issued prior to the commencement of the work, be suspended or revoked the contract shall be terminated immediately and the Contractor shall have no claim against Her Majesty or the Minister as a result of the termination. The Contractor shall be paid for satisfactory work performed up to the time of termination pursuant to the terms of the Contract.
11. The Contractor must comply with the provisions of the:
 - a) Security Requirements Agreement, attached as Annex C; and
 - b) Policy on Government Security <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578>

7.3.2 Contractor's Sites or Premises Requiring Safeguarding Measures

7.3.2.1 Where safeguarding measures are required in the performance of the Work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individuals' sites or premises for the following addresses:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

7.3.2.2 The Company Security Officer must ensure through the [Contract Security Program](#) that the Contractor and individuals hold a valid security clearance at the required level.

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from date of Contract to March 31, 2027 inclusive.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two (2) additional two (2) years periods and two (2) additional one (1) year periods under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least fifteen (15) calendar days before the expiry date of the Contract. The option may only be exercised by the



Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Miriam Britel
Title: Senior Procurement Expert
Indigenous Services Canada
Materiel and Assets Management Directorate
Address: 10 Wellington Street, Gatineau, QC K1A 0H4

Telephone: 873-355-2463
E-mail address: Miriam.britel@sac-isc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.5.2 Project Authority (To Be Determined at Contract Award)

The Project Authority for the Contract is:

Name: _____
Title: _____
Indigenous Services Canada
Address: _____

Telephone: ____ - ____ - _____
Facsimile: ____ - ____ - _____
E-mail address: _____

In its absence, the Project Authority is:

Name: _____
Title: _____
Indigenous Services Canada
Address: _____

Telephone: ____ - ____ - _____
Facsimile: ____ - ____ - _____
E-mail address: _____

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

7.5.3 Contractor's Representative (To Be Determined at Contractor Award)

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone: ____ - ____ - _____
Facsimile: ____ - ____ - _____
E-mail address: _____



7.6 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a [Public Service Superannuation Act](#) (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with [Contracting Policy Notice: 2019-01](#) of the Treasury Board Secretariat of Canada.

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause, "former public servant" is any former member of a department as defined in the [Financial Administration Act](#), R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

- a. an individual;
- b. an individual who has incorporated;
- c. a partnership made of former public servants; or
- d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the [Public Service Superannuation Act](#) (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the [Supplementary Retirement Benefits Act](#), R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the [Canadian Forces Superannuation Act](#), R.S., 1985, c. C-17, the [Defence Services Pension Continuation Act](#), 1970, c. D-3, the [Royal Canadian Mounted Police Pension Continuation Act](#), 1970, c. R-10, and the [Royal Canadian Mounted Police Superannuation Act](#), R.S., 1985, c. R-11, the [Members of Parliament Retiring Allowances Act](#), R.S. 1985, c. M-5, and that portion of pension payable to the [Canada Pension Plan Act](#), R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes () No ()**

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

- a. name of former public servant;
- b. date of termination of employment or retirement from the Public Service.



By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with [Contracting Policy Notice: 2019-01](#) and the [Guidelines on the Proactive Disclosure of Contracts](#).

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** () **No** ()

If so, the Bidder must provide the following information:

- a. name of former public servant;
- b. conditions of the lump sum payment incentive;
- c. date of termination of employment;
- d. amount of lump sum payment;
- e. rate of pay on which lump sum payment is based;
- f. period of lump sum payment including start date, end date and number of weeks;
- g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

7.7 Payment

7.7.1 Basis of Payment – Professional Services

The Contractor will be paid for its costs reasonably and properly incurred in the performance of the Work, in accordance with the Basis of payment in annex B, to a limitation of expenditure of \$ _____ (To Be Determined at Contract Award). Customs duties are included and Applicable Taxes are extra.

7.7.2 Basis of Payment – Maintenance and Support for the Licensed Software

For the Software Maintenance and Support, as detailed in this Contract, Canada will pay the Contractor, the firm annual price(s) set out in Annex B, payable in advance, FOB destination, including all customs duties and applicable taxes are extra.

7.7.3 Limitation of Expenditure

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority.

7.7.4 Method of Payment – Single Payment

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

- a. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- b. all such documents have been verified by Canada;



- c. the Work delivered has been accepted by Canada.

7.7.5 Method of Payment – License Renewal, Maintenance and Support for the Licensed Software

Canada will pay the Contractor in advance for the Work if:

- a. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- b. all such documents have been verified by Canada.

7.7.6 Electronic Payment of Invoices – Contract

The Contractor accepts to be paid using the following Electronic Payment Instrument:

- a) Direct Deposit (Domestic and International);

7.7.7 Discretionary Audit

SACC Manual clause [C0705C](#) (2010-01-11), Discretionary Audit

7.8 Invoicing Instructions

- (a) The Contractor must submit invoices in accordance with the information required in the General Conditions.
- (b) The Contractor's invoice must include a separate line item for each deliverable in the Basis of Payment provision.
- (c) By submitting invoices, the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.
- (d) The Contractor must provide the original of each invoice to the Technical Authority. On request, the Contractor must provide a copy of any invoices requested by the Contracting Authority.

7.9 Certifications and Additional Information

7.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

7.10 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Nova Scotia, New Brunswick, Newfoundland/Labrador and Prince Edward Island.

7.11 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

- (a) the Articles of Agreement;
- (b) the supplemental general conditions:
 - i. [4002](#) (2010-08-16), Supplemental General Conditions – Software Development or Modification Services;
 - ii. [4003](#) (2010-08-16), Supplemental General Conditions – Licensed Software;
 - iii. [4004](#) (2013-04-25), Supplemental General Conditions – Maintenance and Support Services for Licensed Software; and



- iv. 4006 (2010-08-16), Supplemental General Conditions – Contractor to Own Intellectual Property Rights in Foreground Information.

- (c) the general conditions - 2035 (2022-12-01);
- (d) Annex A, Statement of Work;
- (e) Annex B, Basis of Payment;
- (f) Annex C, Security Requirements Check List;
- (g) the Contractor's bid dated _____ (To Be Determined at Contract Award).

7.12 Insurance

SACC *Manual* clause G1005C (2016-01-28), Insurance - No Specific Requirement

7.13 Limitation of Liability

1. This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this section, even if it has been made aware of the potential for those damages.
2. First Party Liability:
 - a. The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:
 - i. any infringement of intellectual property rights to the extent the Contractor breaches the section of the general conditions entitled "Intellectual Property Infringement and Royalties";
 - ii. physical injury, including death.
 - b. The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.
 - c. Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.
 - d. The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (a) above.
 - e. The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:
 - i. any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including Applicable Taxes) for the goods and services affected by the breach of warranty; and
 - ii. any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of _____ times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost" or shown on each call-up, purchase order or other



document used to order goods or services under this instrument), or
\$ _____(To be Determine at Contract Award) .

In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the Contract or \$ _____(To Be Determined at Contract Award) , whichever is more.

- f. If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.
3. Third Party Claims:
- a. Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.
 - b. If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph (a), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.
 - c. The Parties are only liable to one another for damages to third parties to the extent described in this paragraph 3.

7.14 Dispute Resolution

- (a) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.
- (b) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.
- (c) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.
- (d) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "[Dispute Resolution](#)".

7.15 Software Maintenance and Support

- a) **Software Maintenance** (See Annex D for definitions related to this Article): In addition to the Contractor's obligations set out under 4004 - Maintenance and Support Services for Licensed Software, the Contractor must provide the following services as part of the Software Maintenance



throughout the "Software Support Period", which is identified in Annex A, plus any period during which Canada has exercised its option under the Contract to extend the Software Maintenance. The Contractor must provide the Client with the most recent release(s) and version(s) of the Licensed Software during the period of the Software Maintenance, as soon as they are available.

- i. The Contractor must keep track of software releases for the purpose of configuration control.
 - ii. In addition to the Contractor's obligations under Section 3 (Maintenance Releases) of 4004 - Maintenance and Support Services on Licensed Software, the Contractor must deliver the following software code as part of the Software Maintenance:
 - all Bug Fixes, Software Patches, and all other Enhancements;
 - all Upgrades, updates, major and minor New Releases, and Renames;
 - all Extensions and other modifications, including but not limited to drivers, service packs, and Service Releases;
 - all application programming interfaces (APIs), plug-ins, applets and adapters; and
 - all rewrites, including in other programming language(s), where the original version(s) is no longer being maintained by the Software Publisher.
 - iii. The Contractor must continue to maintain the version of the Licensed Software (i.e., the version or "build" originally licensed under the Contract) as a commercial product (i.e. the Contractor or the software publisher must be continuing to develop new code in respect of the Licensed Software to maintain its functionality, enhance it, and deal with Software Errors) for at least five years from the date this Contract is issued. After that time, if the Contractor or the software publisher decides to discontinue or no longer maintain the then-current version or "build" of the Licensed Software and, instead, decides to provide Upgrades to the Licensed Software as part of the Software Maintenance, the Contractor must provide written notice to Canada at least 12 months in advance of the discontinuation.
- b) **Software Support:** In addition to the obligations set out in Supplemental General Conditions 4004, the Contractor must provide the following as part of the "Software Support" throughout the "Software Support Period", which is identified in Annex B, plus any period during which Canada has exercised its option under the Contract to extend the Software Support. The Software Support includes the following Technical Hotline Support and Web Support services:
- i. **Technical Hotline Support:** In addition to the requirements of Supplemental General Conditions 4004 - Maintenance and Support Services on Licensed Software, the Contractor must provide the Technical Hotline Support through the Contractor's toll-free hotline at _____, in English and French, from 8:00 A.M. to 5:00 Eastern Standard Time (EST), Monday to Friday (excluding statutory holidays). The Contractor must answer or return all calls (with a live service agent) within 60 minutes of the initial time of the Client or User's initial call. The Contractor's personnel must be qualified and able to respond to the Client's and any User's questions and, to the extent possible, be able to resolve user problems over the telephone and provide advice regarding configuration problems relating to all deliverables, and related documentation, as well issues relating to installation, configuration and integration of the Licensed Software.
 - ii. **Web Support:** The Contractor must provide Canada with technical Web Support services through a website that must include, as a minimum, frequently asked questions and on-line software diagnostic routines, support tools, and services. The Contractor's website must provide support in English. The Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address is _____.
 - iii. **Email Support:** The Contractor must provide Canada with technical support services through a generic email box. The Contractor must provide answers in the official



language in which the question was requested whichever is applicable. The Contractor must answer or return emails within 24 hours of the initial time of the user's initial email.

7.16 Cloud Services (If Applicable)

7.16.1 Commercially-Available Cloud Services. Canada acknowledges that the Cloud Services are a commercially-available and provided to other customers. As part of the subscription to use the Cloud Services, the Contractor agrees to make available to Canada all the features and functionalities included in the commercially available version of the Cloud Service, and the incidental and required information technology infrastructure services required to deliver the Cloud Services, all of which is included in the subscription price.

7.16.2 Cloud Services Application Evolution; Features or Functionalities. Canada acknowledges that the Cloud Services, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the **commercially available** Cloud Services, with functionality or features and on with terms that are no less favourable than as at the time of Contract award.

7.16.3 Improvements to and Evolution of the Cloud Services. The parties acknowledge that technology and business models evolve quickly and that any Cloud Service provided at the beginning of the Contract Period inevitably will be different from the Cloud Service provided at the end of the Contract Period and the method(s) by which the Cloud Service and any potential peripherals are delivered to Canada are likely to change or evolve and that, at the time of entering into this Contract, the parties cannot possibly contemplate all the Cloud Services that may be delivered under this Contract, other than they will be connected to delivering to Users. With that in mind, the parties agree that:

- The Contractor must maintain and continuously improve the Cloud Service and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide those improvements and enhancements to Canada as part of Canada's subscription, with no price adjustment if those improvements and enhancements are also offered to other customers at no additional cost.
- If the Contractor removes any functions from the commercial offering to the Cloud Services and offers those functions in any new or other Cloud Services or products, the Contractor must continue to provide those functions to Canada as part of Canada's subscription to the Cloud Services, under the existing terms and conditions of the Contract regardless of whether those other Cloud Services or products also contain new or additional functions. Contractor has no obligation to comply with this paragraph if the Cloud Services acquired by Canada is still offered by Contractor in parallel with the new Cloud Services offered to other customers.

7.16.4 Downgrade. If the Contractor is unable to provide the Cloud Services with no less favourable core features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract. The Contractor agrees to immediately repay the portion of any advance payment for the Cloud Services that is unliquidated at the date of the termination to Canada.

7.16.5 SaaS: The Contractor will provide all Services required for Canada to access and use the Cloud Services as specified in Annex A and B.

7.16.6 Commercial Cloud Service Offering. *Canada acknowledges that it will accept the Contractor's commercial Cloud Service offering, and states that, unless explicitly identified as Work or Cloud*



Services to be delivered under this Contract, Canada does not require custom development, alternative services, service levels, functionalities or features.

7.16.7 Authority. The Contractor represents and certifies that it owns or has obtained and will maintain throughout the Contract Period, all necessary authority specifically including intellectual property rights required to provide the Cloud Services in accordance with the terms of this Contract.

7.16.8 Indemnification. The Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any intellectual property infringement claim by a third party based on Canada's use of the Cloud Services.

7.16.9 Usage Grant. The Contractor grants to Canada the non-exclusive, non-assignable right to access and use the Cloud Services from an unlimited number of locations, devices and operating environments, through secure, wireless, mobile or other connection, via the internet, a web browser or other access connection technology which may become available.

7.16.10 Included. The Contractor represents and certifies that the Cloud Services include:

- hosting and maintenance of the Cloud Services,
- provision of all incidental and additional required information technology infrastructure services, in compliance with all required security standards,
- the technical infrastructure that complies with all required security standards, allowing Canada to use the Cloud Services to process any of Canada's Data in compliance with its expressed security standards, and
- unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Cloud Services, all of which is included in the price.

7.16.11 Restricted Usage Rights. Canada acknowledges that in providing the Cloud Services, the Contractor is not delivering ownership rights to any software product, component of the Cloud Services or infrastructure used by the Contractor to provide the Cloud Services, except as expressly provided by written notice. Canada will not knowingly:

- distribute, license, loan, or sell the Cloud Service;
- impair or circumvent the Cloud Service's security mechanisms; or
- remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Cloud Service.

7.16.12 Applicable Terms and Conditions. The Contractor has advised and Canada acknowledges that the Contractor may unilaterally modify the terms under which it provides its commercial offering of the Cloud Services, without notice to its customers, including Canada. The Contractor represents and certifies that any such modification will not result in less favourable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

7.16.13 Additional Terms and Conditions. The parties agree that any terms and conditions, including any "click-through" or "pop-up" notices, that apply to the Contractor's commercial offering of the Cloud Services, including third party tools or incidental infrastructure, will not apply to Canada's use of the Cloud Services if those terms conflict with the express terms of this Contract. The terms and conditions of third party tools not specified in Appendix A are not subject to this section.



7.16.14 Application Programming Interfaces (API): The Contractor must:

- Provide Cloud Services that use open, published, supported, and documented Application Programming Interfaces (API) to support activities such as interoperability between components and to facilitate migration of applications; and,
- Provide a means via API for applications to provision Cloud Services, and extract reporting, billing and financial data pertaining to the Cloud Services consumed by the Client
- Take reasonable measures to protect both internal and external APIs through secure authentication methods. This includes ensuring that all externally exposed API queries require successful authentication before they can be called and providing the ability for the GC to meet the GC's standards on API (<https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html>).

7.16.15 For Cloud Services the Contractor must provide APIs that provide the ability to:

- Interrogate data at rest in Cloud Services; and,
- Assess events and incidents stored in Cloud Service logs.

7.16.16 Service Portal – General

The Cloud Service Provider must provide a secure, web-based, self-service online portal that enables Canada to remotely administer the Cloud Services. This portal must include, at a minimum:

- Service Provisioning;
- Trouble ticketing with email-based notifications;
- Account management and user provisioning including:
- Ability to manage users and associated data; and,
- creating, deleting, and modifying user accounts and permissions;
- Authentication including ability to enable SSO experience;
- Ability to securely access the portal using multi-factor authentication mechanisms to authenticate users;
- Service health or status information including resource usage statistics, reporting on performance, thresholds and alerts; and
- Service state transitions including starting and stopping.

Cloud Service provisioning/de-provisioning must be available via an Application Programming Interface (API). In addition, the Contractor must provide links to documentation, articles, tutorials and guidance in order to help the GC in the use of the API services.

7.16.17 Service Portal Reports

The service must provide the Government of Canada with the ability to generate the following reports:

- Service management reports (e.g. service availability, cost, usage, consumption);
- Asset and configuration management information such as configuration audit reports, configuration change reports, inventory, file integrity monitoring reports, etc.; and
- Help Desk / Service Requests / problem tickets received (service impacting and other), including but not limited to:
 - (i) Number of Tickets opened;
 - (ii) Number of tickets closed;
 - (iii) Average time to respond to Tickets (time between ticket opened and the first contact with customer);
 - (iv) Average time to resolve ticket; and Description of issue.



7.16.18 Master Account Management

The Contractor must ensure the adequate protection of the account management process used to deliver and support the Cloud Services for Canada. Security measures must include, but are not limited to:

- Limiting access to only authorized users who are permitted to execute transactions and functions such as Master account creation and issuance;
- Ensuring the separation of duties of individuals;
- Employing the principle of least privilege, including for specific security functions and privileged accounts;
- Ensuring that authorized users are provided with security awareness and training as part of employment onboarding and when their roles change;
- Creating, protecting, and retaining audit records related to the activities that support account management of Cloud Services provisioned to Canada;
- Providing Canada with reports on audited events for actions related to the issuance and management of Master accounts delivered under the Contract; and
- Ensuring that Canada's Data is protected during and after personnel actions such as terminations and transfers.

7.16.19 Language of Choice

The Contractor of the Commercially Available Public Cloud Service must provide the ability for the GC to choose the official language of their choice, French or English, when browsing, ordering and contacting the Cloud Service Provider. The Contractor must provide these Cloud Services directly and not through a partner, reseller, agent or other representative. This includes but is not limited to the following:

- Browsing the service(s) on their website(s);
- Ordering Cloud Services;
- Contacting the company for assistance via phone, email or chat.
- Ability for Canada to request technical or support documentation in their language or choice.



ANNEX "A"

STATEMENT OF WORK

Atlantic Electronic Dental Records System

1. SCOPE

1.1. Introduction

Indigenous Services Canada (ISC), a department of the Government of Canada, has a requirement for the implementation of an Electronic Dental Records (EDR) system for the collection, management, storage, and sharing of dental patient data and information.

It is to be delivered as a Software as a Service (SaaS) on a cloud that is capable of handling Protected B data.

Community Oral Health Services Atlantic (COHS ATL) of Indigenous Services Canada's First Nations and Inuit Health Branch in the Atlantic region (ISC FNIHB ATL), is planning the implementation of an Electronic Dental Records (EDR) system for the collection, management, storage, and sharing of dental patient data and information. The EDR system will replace the paper-based dental records currently in use across all Indigenous community dental clinics in the four Atlantic provinces of Nova Scotia, New Brunswick, Newfoundland/Labrador and Prince Edward Island.

The scope of this procurement encompasses:

- An Electronic Dental Records system as a SaaS type of service.
- Professional services required for its implementation and rollout.
 - Training service
Canada requires the Contractor to provide training to 5 users at ISC, to start, that is comprehensive enough as to enable them to perform administrative functions, general use of the system and testing.
 - Configuration services
Canada requires the Contractor to provide professional services for modifying and the configuring of the EDR system as required to meet organizational needs.
 - Rollout services
Canada requires the Contractor to provide professional services for the rollout of the EDR system at all community dental clinic sites, as well as training for up to 10 additional users.
- Provision of Technical Support services/Helpdesk Services for duration of contract.
- Ongoing support services for training, on an as needed basis

1.2. Objectives of the Requirement

The implementation of an EDR system by COHS ATL will be an effective way of mitigating the barriers associated with paper-based dental records. Within the field of dentistry, EDR is the widely accepted industry standard for the secure collection, management, storage (including digital x-rays), and sharing of patient information. There are many potential benefits associated with EDR systems, including the following:

1. Improved patient care and safety because of rapid access to and point of care entry of comprehensive patient data,
2. More efficient management of appointment scheduling, patient data, and resources,
3. Enhanced communication with patients, consulting providers, pharmacies and legal personnel, and
4. Increased security for patient data storage.



COHS ATL has identified the need to implement an EDR system with the following digital capabilities:

1. Entry of and access to Protected B patient information, including, but not limited to, demographic information, dental patient data, digital radiographs, as well as digitized historical patient records,
2. Management of appointment scheduling, patient data and resources,
3. Secure digital storage of personal patient information including digital x-rays,
4. Sharing of patient data and information between authorized parties,
5. Collation of patient data for program/service evaluation and legal matters, and
6. Interface with current and new digital x-ray systems.

Atlantic EDR System Project outcomes are anticipated to be as follows:

1. Modernization of COHS ATL dental record keeping methods to current gold standard through the selection and implementation of an EDR system,
2. Improved patient service and outcomes,
3. Mapping of critical business processes as related to EDR system use,
4. Training of authorized users, and
5. Continued maintenance of EDR System.

1.3. Background

COHS ATL provides dental services to Indigenous communities throughout the Atlantic region. Currently, Oral Health Care Providers (OHCPs) note patient information and document services rendered in paper-based charts. These paper charts are stored in various sites across the region, depending on the location of community dental clinics. This mode of logging and storing patient data is becoming increasingly problematic for several reasons:

1. Storage capacity for paper dental records is being exceeded at all clinic sites. Current storage methods are outdated and insecure – a fire or flood at any community clinic location could potentially result in the permanent loss of important patient information.
2. Digital radiography (i.e., digital dental x-ray system) is being used in all community dental clinics, necessitating the storage of a patient's digital dental x-rays separate from their paper dental chart. As a result, gathering a comprehensive picture of a patient's dental status is more challenging. The storage of digital dental x-rays involves a combination of shared and local drives, leaving this important information vulnerable to loss and mismanagement.
3. Patient data is difficult to collate for the purpose of program monitoring, oral health outcome evaluation and legal proceedings.
4. Access to stored patient information is limited to those on site. As such, consultation with colleagues not residing in community and the sharing of patient information with authorized parties in a secure manner present many challenges.

1.4. Specific Scope of the Requirement

Comprehensive dental records are critical to the practice of dentistry. The maintenance of accurate dental records is essential for quality patient care and follow-up. They also play an important role in forensic identification and legal matters. Historically, dental records have been paper-based. However in this digital era, the vast majority of dental practices employ an EDR system for the collection, management, storage, and sharing of patient data and information. The adoption of an EDR system by COHS ATL will be an effective way of mitigating the barriers associated with paper-based dental records.



- The EDR system must be implemented by March 2023.
- The EDR system should be configured as detailed in Table 1.1 for authorized users.

Table 1.1 Authorized Users and Roles

Roles/Users	Access Rights
Administrators (Regional Dental Officer, Dental Therapy Manager and COHI Co-ordinator)	This category of users has the ability to: <ul style="list-style-type: none"> • Access administrative rights • Create electronic dental records • Read electronic dental records • Digitally sign electronic dental records <ul style="list-style-type: none"> • Manage system access • Run reports
FNIHB Atlantic Regional Health Services: Super Users (Dental Therapists and other licensed oral health care professionals [i.e., Dental Hygienists and Dentists])	This category of users has the ability to: <ul style="list-style-type: none"> • Create electronic dental records • Update electronic dental records • Digitally sign electronic dental record entries
Read Only Users	This category of users has the ability to: <ul style="list-style-type: none"> • Read only

2. REQUIREMENTS

Atlantic EDR System requirements are divided into four sections: Business Requirements (Table 2.1), Non-Functional Requirements (Table 2.2), Functional Requirements (Table 2.3) and Technical Scalability Requirements (Table 2.4). Unless otherwise stated, it is to be assumed that all records of services and/or activities should include the identity of the person(s) responsible, as well as the date, time and location of the activities and/or services rendered.

COHS ATL will have exclusive access to the Atlantic EDR System described herein. However, the long term goal of this project is to put in place an EDR system that can be easily adapted and implemented in other regions. COHS HQ is a stakeholder of the Atlantic EDR System Project.

Table 2.1 Business Requirements of Atlantic EDR System

Priority: M=Mandatory, HD=Highly Desirable, D=Desirable

Ref. #	Business Requirement	Priority
REQ-001	System must be modifiable and configurable to meet needs of organization.	M
REQ-002	System must be deployable using Cloud technology able to be accredited to Government of Canada Protected B Security Profile.	M



REQ-003	System must interface/link with current and new digital radiography systems.	M
REQ-004	System must provide remote, point-of-care access to dental records.	M
REQ-005	Must have different levels of approved access to EDR system.	M
REQ-006	System must have the ability to print hard copies of dental records.	M
REQ-007	System must have the ability to run reports for service and program evaluation.	M
REQ-008	System must have the ability to upload digitized copies of paper-based dental records and existing digital x-ray files into EDR system as required.	M
REQ-009	System must have the ability to upload scanned letters from external providers (e.g., dental specialists, physicians).	M

Table 2.2 Non-Functional Requirements of Atlantic EDR System

Priority: M=Mandatory, HD=Highly Desirable, D=Desirable

Category	Ref. #	Requirement	Priority
Availability	NFR-1	Contractor must provide support during business hours Monday to Friday, from 8:00 am to 5:00 pm Atlantic Standard Time.	M
	NFR-2	Contractor must provide published Service Level Agreement for the proposed system. The included service level commitments must provide ISC with warranty, maintenance and support services. Support services should be provided in the language of user's choice of either English or French and may be delivered by telephone, e-mail, mobile messaging or web-based tools, as best applicable. The agreement must be signed and becomes binding prior to system launch.	M
	NFR-3	System must include the capability for users to report and track issues, either online or through telephone support.	M
Capacity	NFR-4	Processing and storage capabilities of the system must have the ability to adapt and support increasing amount of data and increasing number of users.	M
	NFR-5	System must support a minimum of 25 active/concurrent users.	M
	NFR-6	System must support creation and management of approximately 25,000 records per year.	M
	NFR-7	System must upload .pdf, .doc, .docx, .jpg files, x-rays, and other relevant formats to support the dental office operation.	M



	NFR-8	System must allow for file size up to 10 megabytes without warning and attachments of size larger than 10 megabytes should trigger a warning to the user.	M
	NFR-9	System must have encrypted Cloud-based data storage.	M
	NFR-10	System must allow uploading of colored intra-oral and facial photos or any other relevant information required for patient files.	M
Compliance	NFR-11	System must comply or can be modified to comply with <i>Official Languages Act</i> by being functionally equivalent in English and French and must allow users to work in the Canadian official language of their choice. Official Languages Act is here: Official Languages Act	M
	NFR-12	System must comply with Government of Canada standards on accessibility and usability. Must meet the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 .	M
	NFR-13	System must meet all of the Government of Canada policies on Service and Digital Standards.	M
	NFR-14	System must comply with Security Requirements for the secure handling, processing and storing of Protected B information.	M
	NFR-15	System must adhere to IM requirements (i.e., retention period and disposition).	M
	NFR-16	System Browser Configuration: c) for Internet based user interfaces, all user interfaces must be compatible with the standard ISC Internet browsers (Chrome, Edge, etc.) at the time the system is deployed to production and be kept current with subsequent versions when ISC upgrades to a new standard Internet browser, at no additional cost. d) for public facing Internet sites, all user interfaces must be compatible with the latest minus 2 versions of the approved ISC browsers, Chrome, Edge, and Safari.	M
Data Integrity	NFR-17	System must incorporate input validation.	M
	NFR-18	System must incorporate data validation.	M
	NFR-19	System must have the ability to remove duplicate data.	M
	NFR-20	System must incorporate Government of Canada-approved backup and restore functionality. The System must, on a daily basis, back up all ISC user credentials, data and files (e.g., audit records, documents, contact lists) onto a backup system, stored at a different location from the primary data center. Backups must also be stored within Canadian borders and encrypted.	M



	NFR-21	System must provide access controls.	M
	NFR-22	System must provide audit trail. Actions to be logged such as: <ul style="list-style-type: none"> • File creation • File deletion • Modifications • Logon/logoff information 	M
Radiography Integration	NFR-23	System must interoperate with digital radiography system.	M
Maintainability / Supported Technology	NFR-24	System must be designed using current technologies, frameworks and coding languages that will continue to be supported by Contractor/User Community for the duration of EDR system's expected lifespan.	M
Performanc e	NFR-25	System must respond to commands within 3 seconds under normal operating conditions.	M
	NFR-26	System must ensure that when a user performs a Logoff, or when a user is idle for a set period of time, the respective user session is terminated.	M
Recoverability	NFR-27	System must restore data in the event of a failure (i.e., EDR system is capable of restoring all data saved prior to point of failure).	M
	NFR-28	System must have a recovery time of 24 hours in the event of a failure (i.e., EDR system capable of recovering within 24 hours).	M
	NFR-29	Contractor must provide a Disaster Recovery Plan (DRP).	M
Reliability	NFR-30	System must be available 99% of the time, 7 days a week.	M
Security	NFR-31	System must meet all applicable ISC/CIRNAC security and privacy requirements. Must ensure adequate protection of data according to IT standards for Protected B information. See: ANNEX A – Tier 2 (Information categorized Up to and including Protected B) SECURITY REQUIREMENTS PRECEDENT TO CONTRACT AWARD FOR SOFTWARE AS A SERVICE CONTRACTS	M



	NFR-32	System must be able to provide required evidence to successfully meet Protected B accreditation.	M
Transition	NFR-33	System must have ability to upload digitized copies of paper-based dental records.	M
	NFR-34	System must have ability to upload existing digital x-ray files as required and sync with appropriate patient records.	M
	NFR-35	The Contractor is required to provide READ Access and privileges to the ISC DBA team, in order to perform the required data extraction or duplication from the Contractor-system database into the departmental infrastructure premises.	M
Usability	NFR-36	Contractor has comprehensive training plan to ensure ease of use and learning of the system based on user needs.	HD
Training	NFR-37	Contractor has ongoing support services for training, on an as needed basis.	HD

Table 2.3 Functional Requirements of Atlantic EDR System

Priority: M=Mandatory, HD=Highly Desirable, D=Desirable

Category	Ref. #	Requirement	Priority
Administrative Functions	FR-1	System must allow users with Administrator permissions to add/modify/delete Electronic Dental Records (EDRs). Must offer ISC Administrators and Coordinators the capability to manage user access control (including privacy) and permission settings.	M
	FR-2	Privacy settings of the system must have the ability to restrict viewing permissions of employee data based on organizational structure.	M
Audit Tracking	FR-3	System must be able to record users' name, role and responsibilities to maintain accurate historical audit trail.	M
	FR-4	System must be able to record all accesses to client data.	M
	FR-5	System must support two factor authentication.	M
	FR-6	System must allow modification of X-Number to Status Number (SN) in a client's record if client receives SN after their initial visit. Contractor must allow the addition/modification of SNs to a record by Administrators only. [SN is derived from the Status Verification System (SVS). The function of the SVS system is to provide Status Numbers to Clients regarding their eligibility to use the services provided.]	M
	FR-7	System must allow access to approved external users (i.e., non-Internal/non-GoC users).	M



Authorization Levels	FR-8	System must allow configuration of the roles as outlined in Table 1.1 Authorized Users and Roles of the SOW.	M
	FR-9	System must not allow deletion or modification of digitally signed entries or records.	M
Business Rules	FR-10	System must allow saving and signing.	M
	FR-11	System must have the ability to auto save.	M
	FR-12	System must ask the user to verify signature.	M
	FR-13	System must provide a reminder if user leaves an entry/record digitally unsigned.	M
	FR-14	System must store metadata with the Electronic Data Record.	M
	FR-15	System must allow disposition rules for records management.	M
	FR-16	System must allow searching of data records by last name, first name, gender, date of birth or Status Number/X-Number.	M
	FR-17	System must allow for remote, point of care access to electronic dental records.	M
Data Records	FR-18	System must be a cloud-based, Software as a Service (SaaS) solution that can manage Protected B information.	M
	FR-19	System must be deployable across four Atlantic provinces.	M
	FR-20	System must provide charts that cover a lifetime of activity.	M
	FR-21	System must be able to upload digitized copies of paper consent forms, letters from specialists, etc. and link them to the appropriate client electronic dental record.	M
	FR-22	System must store digital radiography files and link to appropriate client electronic dental record.	M
	FR-23	System must have client odontogram as a feature.	M
	FR-24	System must allow recording of treatment notes.	M
	FR-25	System must display daily appointment schedule.	M
	FR-26	System has the ability to send email notifications to clients (e.g., appointment reminders).	HD



	FR-27	System must allow entry of a unique identifier (eg. Status Number, X-Number) to each client electronic dental record.	M
External Interfaces (User Interfaces)	FR-28	System must interface/link with current and new digital radiography systems.	M
	FR-29	System must be able to connect to a printer and allow printing of required sections of EDRs.	M
	FR-30	System must be able to connect to a scanner and allow scanning, as well as uploading of scanned material.	M
Reporting	FR-31	System must have ability to generate reports for service evaluation.	M
	FR-32	System must have ability to generate reports for program evaluation.	M

Table 2.4 Technical Scalability Requirements of Atlantic EDR System

Priority: M=Mandatory, HD=Highly Desirable, D=Desirable

Category	Ref. #	Requirement	Priority
Scalability	TCR-1	System must be scalable to meet National growth.	M
	TCR-2	System must be expandable for implementation across Canada.	HD

2.1. Tasks, Activities, Deliverables and Milestones

Table 2.5 Tasks, Activities, Deliverables and Milestones

Deliverable Title	Deliverable Description	Deliverable Type
Project Kickoff and Progress Meetings	Contractor will lead/chair a project kick-off meeting, as well as regular project meetings where they will discuss and agree on how the project will be run, the listed deliverables and the schedule. Kick-Off meeting should occur no later than 10 business days after contract signing.	Meetings



Training Plan	<p>Plan must ensure that training is comprehensive enough so that Canada trainees are, at a minimum, enabled to:</p> <ul style="list-style-type: none">i. Use all functional and administrative features;ii. Understand the process to migrate the paper-based assets. <p>The Contractor will propose the best and alternative ways of providing training, with respect to the location of staff in Atlantic Canada.</p> <p>If training is not sufficient, an approval process can be recommended.</p>	Document
Implementation Plan	<p>Plan must describe how the Contractor envisages all activities pertinent to implementation, not limited to the following:</p> <ul style="list-style-type: none">i. Creation of various environments (i.e.: test, prod etc.);ii. Creation of system access for the users;iii. Configuration and tuning of the system;iv. Migration of Canada's paper-based information assets to the system;v. Incorporation of digital x-ray files into EDR System;vi. Design and implementation of business processes as needed;vii. EDR system to be implemented all at once, across the Atlantic region. <p>Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.</p>	Document
Security Assessment and Authorization Process	<p>Canada's Security Assessor will lead the Security Assessment process that will include:</p> <ul style="list-style-type: none">i. Definition of Statement of Sensitivity;ii. Definition of the Security Control profile;iii. Evidence Gathering and;iv. Write the Security Assessment and Authorization Report. <p>The Contractor must provide required evidence to support the risk management process.</p>	Meetings and Documents



Testing Plan	<p>Plan must describe how the Contractor envisages at least the following activities:</p> <ul style="list-style-type: none"> i. Definition and setup of all offered testing environments; ii. Definition of offered types of testing (e.g., functional, performance) and identification of the roles (Contractor and Canada) for each type of testing; iii. Definition of Test Cases and the estimated timing of their execution. <p>Upon contract award, the Contractor and Canada may need to make updates before Canada accepts the final plan.</p>	Document
Core Training	<p>Guided by the Training Plan, the Contractor must train up to 15 core users, including Administrators and Super Users who would then be able to perform functional and performance testing as well as general use of the system.</p>	Professional Services
Testing - Functional and Performance	<p>Guided by the Test Plan, the Contractor must:</p> <ul style="list-style-type: none"> i. Set up testing environments for functional and performance testing; ii. Be available to Canada, and assist if required, in troubleshooting the functional and performance testing of the system. <p>Contractor's designated resources qualified to support Canada with regard to testing will be called upon only if Canada faces issues they cannot resolve themselves.</p>	Professional Services
Go Live	<p>The Contractor must support Canada, as and when required, in putting the system live in production as per the defined project schedule.</p>	Professional Services

2.2. Specifications and Standards

The Contractor must provide his own development environment. ISC will perform user testing in ISC test environments against the Contractor test environment. The Government of Canada will be responsible for the costs of computer equipment, operating systems, and database licenses used to host the ATL EDRS.

The standards required by Shared Services Canada are as follows:

- The contractor will provide information as required to the Contracting Authority or an authorized representative to ensure that the system complies with Government of Canada security standards.
- The Atlantic EDRS must comply with IT specifications supported by Shared Services Canada (SSC)

The Contractor must warrant that the new system will function without defect and according to requirements specified by ISC for a minimum of 90 business days free of charge. As part of the warranty, the Contractor must determine the cause of any defect, analyze the impact/risk to the overall system by repairing any defect, test and implement a solution, and update all associated documentation.

The Contractor must respond to warranty requests within one business day and be prepared to perform the work at the same time, unless otherwise agreed to in writing by the Contracting Authority. The



warranty period will start after the Contractor has received confirmation in writing from the ISC Contracting Authority that the work associated with this contract has been accepted as completed.

Throughout the contract, the resource must execute the aforementioned tasks and complete assigned deliverables in a timely and quality manner. All deliverables are subject to the review and approval of the Contracting Authority.

2.3. Technical, Operational and Organizational Environment

The system will be used within the FNIHB Atlantic regional offices and ISC community dental clinics across the region by OHCPs, one clinic of which is situated in a remote area.

2.4. Method and Source of Acceptance

Payment of the fees will be made upon the Contractor's completion of tasks as evidenced by the production of the specified Deliverables. Payments will be made only after receipt of such Deliverables and acceptance thereof by the Contracting Authority.

The final work will be accepted when the Contractor has completed all of the requirements indicated in the Statement of Work, Canada has reviewed the documents and asked for changes if needed, and the ISC Contracting Authority has signed off and approved the system and accompanying documentation as being completed and accurate based on the requirements set forth by ISC.

Except as otherwise specifically provided for herein, ISC will not be required to pay for partially completed tasks or for any additional work that may be required that the Contractor has not budgeted for in its proposal.

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work, unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

2.5. Reporting Requirements

Performance or Status Reporting Requirements

The Contractor must participate in status meetings every two weeks and must submit progress reports in MS Word to the Technical Authority by email.

The progress reports must be provided prior to each status meeting or as required by Canada.

The progress reports do not have a standard format requirement, however, they are expected to provide information on:

- Work completed during the reporting period;
- Status update on the activities underway;
- Planned activities for the next period; and
- Assessment of risks and a proposed mitigation strategy: any areas of concern pertinent to the contract, such as difficulties encountered in carrying out the work plan, possible solutions and other important issues impacting the project.

The contractor must run reports for service and program evaluation.

The Contractor must notify the Contracting Authority immediately if any issues arise that may impact the project schedule (Table 4.1) and their ability to deliver the work as described in Table 2.5.



The Contractor must meet with Canada's representatives to present and review the system prior to the Contracting Authority signing off and accepting the final deliverables of the contract.

2.6. Project Management Control Procedures

The individual identified in the proposal as the Project Authority or Technical Authority will:

- Maintain ultimate accountability for the outcome of the project;
- Champion the project from a business perspective;
- Remove obstacles, resolve conflicts and assist with issues & risks that have been escalated;
- Chair the Steering Committee;
- Secure funding and resources as necessary;
- Endorse the project as a value investment to the region;
- Make decisions that are beyond the authority of the PM; and
- Sign-off on major deliverables.

3. ADDITIONAL INFORMATION

3.1. Canada's Obligations

N/A

3.2. Contractor's Obligations

- Unless otherwise specified, the Contractor must use its own equipment and software for the performance of this Statement of Work.
- Title to the equipment/furnishings charged against this Contract shall vest in Canada upon payment of invoiced amounts and must remain so vested at all times.
- For each item of equipment/furnishings that is purchased, the Contractor is to record the name, manufacturer, model number, serial number, optional equipment, Contractor and price and forward this information to the Project Authority.
- The Contractor must label all equipment/furnishings as being the property of Canada.
- Notwithstanding the fact that the equipment/furnishings under this Contract become vested in Canada, the equipment/furnishings must remain within the custody and control of the Contractor until such time as the Project Authority provides instructions for its delivery. During this period of time, the Contractor must take reasonable and proper care of the equipment/furnishings.

3.3. Location of Work, Work Site and Delivery Point

The work must be carried out on the premises of the Contractor, although meetings will be held virtually and technical access/training may require alternate sites within the Atlantic Region.

Due to security restrictions, the Contractor will not be granted remote access to the ISC network.

3.4. Language of Work

The language of work and documentation must be in English.

3.5. Insurance Requirements

The Contractor must obtain and maintain an appropriate level of professional liability insurance coverage.

3.6. Travel and Living



Payment for travel and living expenses must be made in accordance to the terms of payment and the National Joint Council Travel Directive. Travel may be required.

4. PROJECT SCHEDULE

4.1. Schedule and Estimated Level of Effort (Work Breakdown Structure)

Activity	Date
Configuration	All activities to be completed by March 31st, 2023
Security Deliverables, Authority to Operate	
UAT Testing	
Train Users	
Go Live	
Implementation Close-Out	

5. REQUIRED RESOURCES OR TYPES OF ROLES TO BE PERFORMED

The Contractor must provide a project manager or account representative to coordinate basic project implementation and progress, as required.



ANNEX “B”

BASIS OF PAYMENT

Table 1: Initial Period – From Contract Award Date to March 31, 2027

Item No.	Description	Unit of Measure	Estimate Quantity	Unit Price (\$CAD)	Price (\$CAD)
1	Solution and Implementation	Unit	1	\$TBD	\$TBD
2	Software License, Software Hosting, Maintenance and Support – Fiscal Year 2022-2023	Users	25	\$TBD	\$TBD
3	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2023-2024	Users	25	\$TBD	\$TBD
4	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2024-2025	Users	25	\$TBD	\$TBD
5	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2025-2026	Users	25	\$TBD	\$TBD
6	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2026-2027	Users	25	\$TBD	\$TBD
Sub-Total:					\$TBD

Table 2: Option Period 1 – From April 01, 2027 to March 31, 2029

Item No.	Description	Unit of Measure	Estimate Quantity	Unit Price (\$CAD)	Price (\$CAD)
1	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2027-2028	Users	25	\$TBD	\$TBD
2	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2028-2029	Users	25	\$TBD	\$TBD
Sub-Total:					\$TBD

Table 3: Option Period 2 – From April 01, 2029 to March 31, 2031

Item No.	Description	Unit of Measure	Estimate Quantity	Unit Price (\$CAD)	Price (\$CAD)
1	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2029-2030	Users	25	\$TBD	\$TBD
2	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2030-2031	Users	25	\$TBD	\$TBD



Sub-Total:	\$TBD
------------	-------

Table 4: Option Period 3 – From April 01, 2031 to March 31, 2032

Item No.	Description	Unit of Measure	Estimate Quantity	Unit Price (\$CAD)	Price (\$CAD)
1	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2031-2032	Users	25	\$TBD	\$TBD
Sub-Total:					\$TBD

Table 5: Option Period 4 – From April 01, 2032 to March 31, 2033

Item No.	Description	Unit of Measure	Estimate Quantity	Unit Price (\$CAD)	Price (\$CAD)
1	Software License Renewal, Software Hosting Renewal, Maintenance and Support – Fiscal Year 2032-2033	Users	25	\$TBD	\$TBD
Sub-Total:					\$TBD



ANNEX "C"

SECURITY REQUIREMENTS CHECK LIST

Affaires autochtones et Développement du Nord Canada / Aboriginal Affairs and Northern Development Canada	Contract Number / Numéro du contrat 1000244928
	Security Classification / Classification de sécurité Unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A – CONTRACT INFORMATION / PARTIE A – INFORMATION CONTRACTUELLE																																																																							
1. Branch / Sector / Directorate / Region / Direction générale / Secteur / Direction / Région ISC - FNIHB - ATL Region	2. Contract type / Type de contrat Non-Competitive / Non-compétitif <input type="checkbox"/> Competitive / Compétitif <input checked="" type="checkbox"/> Type:																																																																						
3. Brief Description of Work / Brève description du travail Community Oral Health Services-Atlantic (COHS-Atlantic) is proposing the implementation of an Electronic Dental Records (EDR) System for the collection, management, storage, and sharing of patient data and information.																																																																							
4. Contract Amount / Montant du contrat 400,000 \$	5. Company Name and Address (for non-competitive contract only) / Nom et adresse de la compagnie (pour les contrats non-compétitifs seulement):																																																																						
5. Contract Start and End date / Date de début et de fin du contrat 2022-09 to / au 2026-03																																																																							
7. Will the supplier require / Le fournisseur aura-t-il : 7.1 access to PROTECTED and/or CLASSIFIED information or assets? / accès à des renseignements ou à des biens désignés PROTÉGÉS et/ou CLASSIFIÉS? <input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui 7.2 an access card to AANDC premises? / besoin d'une carte d'accès aux bureaux d'AANDC? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui 7.3 access to the departmental computer network? / accès au réseau informatique du Ministère? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui (If the answer is No to all three questions, go to Part D / Si la réponse est Non aux trois questions, aller à la Partie D)																																																																							
PART B – SAFEGUARDS OFF-SITE (COMPANY) / PARTIE B – MESURES DE PROTECTION À L'EXTÉRIEUR (COMPAGNIE)																																																																							
PHYSICAL INFORMATION / ASSETS / RENSEIGNEMENTS MATÉRIELS / BIENS 8. Will the supplier be required to receive/store PROTECTED and/or CLASSIFIED information/assets on its site or premises? / Le fournisseur sera-t-il tenu de recevoir/l'entreposer sur place des renseignements/biens PROTÉGÉS et/ou CLASSIFIÉS? <input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui																																																																							
INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI) 9.1 Will the supplier be required to use its computers, portable media, or IT systems to electronically process/store sensitive information? / Le fournisseur sera-t-il tenu d'utiliser ses propres ordinateurs, médias portatifs ou systèmes TI pour traiter/stocker électroniquement des renseignements sensibles? <input type="checkbox"/> No / Non <input checked="" type="checkbox"/> Yes / Oui 9.2 Will the supplier be required to electronically transmit sensitive information to/from the Department or with other parties? / Le fournisseur sera-t-il requis de transmettre électroniquement de l'information sensible au/à partir du Ministère ou avec d'autres parties? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui If yes, specify: / Si oui, spécifiez: a) Email transmission / Transmission par courrier électronique: <input type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui b) Other transmission (Secure FTP, Collaboration, etc) / Autre transmission (FTP sécurisée, collaboration, etc): <input type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui c) Remote access required to AANDC network (VPN, Citrix) / Besoin de connexion à distance au réseau d'AANDC (VPN, Citrix): <input type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui 9.3 Will the supplier be required to safeguard COMSEC* information or assets? / Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC*? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui * Handling equipment and measures for secure transmission and emission (cryptographic, secure fax/phone) / Manipulation de l'équipement et des mesures sécuritaires pour fin de transmission et émissions (cryptographie, téléphone/télécopieur sécurisé)																																																																							
10. SUMMARY CHART / TABLEAU RÉCAPITULATIF <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th rowspan="2">Category / Catégorie</th> <th rowspan="2">Please refer to question / Veuillez vous référer à la question:</th> <th colspan="3">PROTECTED / PROTÉGÉ</th> <th colspan="3">CLASSIFIED / CLASSIFIÉ</th> </tr> <tr> <th>A</th> <th>B</th> <th>C</th> <th>CONFIDENTIAL / CONFIDENTIEL</th> <th>SECRET</th> <th>TOP SECRET / TRÈS SECRET</th> </tr> </thead> <tbody> <tr> <td>Information Assets / Renseignements/biens</td> <td>8.1</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Information Assets off site / Renseignements/biens (autrement)</td> <td>8</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>IT Information Assets off site / Renseignements/biens TI (autrement)</td> <td>9.1</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>IT Transmission – source / Transmission TI – source</td> <td>9.2 a)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>IT Transmission – other / Transmission TI – autre</td> <td>9.2 b)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Remote Access to Network / Connexion à distance au réseau</td> <td>9.2 c)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>COMSEC</td> <td>9.3</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Category / Catégorie	Please refer to question / Veuillez vous référer à la question:	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	Information Assets / Renseignements/biens	8.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Information Assets off site / Renseignements/biens (autrement)	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IT Information Assets off site / Renseignements/biens TI (autrement)	9.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IT Transmission – source / Transmission TI – source	9.2 a)	<input type="checkbox"/>	<input type="checkbox"/>					IT Transmission – other / Transmission TI – autre	9.2 b)	<input type="checkbox"/>	<input type="checkbox"/>					Remote Access to Network / Connexion à distance au réseau	9.2 c)	<input type="checkbox"/>	<input type="checkbox"/>					COMSEC	9.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Category / Catégorie	Please refer to question / Veuillez vous référer à la question:			PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ																																																																
		A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET																																																																
Information Assets / Renseignements/biens	8.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																																
Information Assets off site / Renseignements/biens (autrement)	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																																
IT Information Assets off site / Renseignements/biens TI (autrement)	9.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																																
IT Transmission – source / Transmission TI – source	9.2 a)	<input type="checkbox"/>	<input type="checkbox"/>																																																																				
IT Transmission – other / Transmission TI – autre	9.2 b)	<input type="checkbox"/>	<input type="checkbox"/>																																																																				
Remote Access to Network / Connexion à distance au réseau	9.2 c)	<input type="checkbox"/>	<input type="checkbox"/>																																																																				
COMSEC	9.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																																
PART C – PERSONNEL / PARTIE C – PERSONNEL																																																																							
11.1 Personnel Security Screening Level Required: / Niveau d'enquête de la sécurité du personnel requis: <input type="checkbox"/> N/A / Non requis <input checked="" type="checkbox"/> Reliability / Fiabilité <input type="checkbox"/> Confidential / Confidentiel <input type="checkbox"/> Secret <input type="checkbox"/> Top Secret / Très secret																																																																							
11.2 May unscreened personnel be used for portions of work? / Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui <input type="checkbox"/> N/A / Non requis																																																																							
12. Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED? / La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui																																																																							



Contract Number / Numéro du contrat
100034628
 Security Classification / Classification de sécurité
 Unclassified

PART D – AUTHORIZATION / PARTIE D – AUTORISATION			
13. Organization Project Authority / Chargé de projet de l'organisme			
Name (print) – Nom (en lettres moulées) Sandra Musgrave		Title - Titre Director of Primary Care	Signature musgrave, sandra
Digitally signed by musgrave, sandra Date: 2022.12.29 12:28:08 -0500			
Telephone No. – N° de téléphone +1 (902) 426-0335	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel sandra.musgrave@sac-isc.gc.ca	Date
14. Organization Security Authority / Responsable de la sécurité de l'organisme			
Name (print) – Nom (en lettres moulées) Marc-André Trottier		Title - Titre Contract Security Officer	Signature trottier, marcandre
Digitally signed by trottier, marcandre Date: 2022.12.30 09:35:56 -0500			
Telephone No. – N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel marc-andre.trottier@sao-isc.gc.ca	Date 2022-12-30
15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui			
16. Procurement Officer / Agent d'approvisionnement			
Name (print) – Nom (en lettres moulées) Miriam Briél		Title - Titre Senior Procurement Expert	Signature britel, miriam
Digitally signed by britel, miriam Date: 2022-12-13 10:15:28			
Telephone No. – N° de téléphone 873-355-2463	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel miriam.briel@sao-isc.gc.ca	Date December 13, 2022
17. Contracting Security Authority / Autorité contractante en matière de sécurité			
Name (print) – Nom (en lettres moulées) Marc-André Trottier		Title - Titre Contract Security Officer	Signature trottier, marcandre
Digitally signed by trottier, marcandre Date: 2022.12.30 09:35:56 -0500			
Telephone No. – N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address – Adresse courriel marc-andre.trottier@sao-isc.gc.ca	Date 2022-12-30



Security Requirements Agreement

Company name: _____
 Request for proposal: 1000244928
 Contract: _____

1. Physical Security Transportation and Safeguard Requirements

It is important to properly safeguard sensitive information. This will assist in reducing the risk of unauthorized access, disclosure or compromise of **Sensitive** information.

1.1 Physical Safeguards:

The Protected documents must be safeguarded in a locked security container with access restricted to the contractor only.

	Protected A	Protected B
Container	Key locked container	Dial lock container
Facility	Restricted access room within office/home	Restricted access room within office/home

Definitions:

Protected information: Information for which unauthorized disclosure, destruction, interruption, removal or modification could reasonably be expected to cause injury to an individual, organization or government which lies outside the national interest.

Protected A: Could cause injury. A few examples: Personal data such as names, birth dates, home address and telephone number, linguistic profiles, salary figures, Social Insurance Numbers.

Protected B: Could cause serious injury. A few examples: Several Protected A information compiled, business or client information such as: commercial financial, scientific, or technical information, loss of competitive advantage, legal opinion, medical record.

1.2 **Transportation**

1.2.1 Transportation of Paper Records:

- **Protected** documents must be securely packaged in folders carried in an approved locked briefcase.
- Sensitive information must be kept under the constant control of the contractor, including during meals and during travel.
- While on contractor premises, portable media devices containing sensitive information are equivalent to paper records and are to be physically stored within an appropriate security container such as those listed above.

1.2.2 Prevention Tips While in Transit:

- Prior to travel: Make an inventory of information.
- Public Areas: Sensitive information must never be read, displayed, discussed or used in public areas.
- Overnight Stopovers: Information is not to be left unattended.
- Travelling by Car: Locked in trunk while travelling. Never to be left unattended in vehicle.



- Travelling by Air: Bring with you as a carry-on.
- Hotels/Conference Centers: Be careful about sensitive conversations in hotel conference rooms.
- Never use hotel reception staff or devices to fax, receive or copy sensitive information. Ensure all participants have the proper security clearance and the need-to-know.
- In the event a device or a document is lost or stolen, it must be reported immediately to the Department.

1.2.3 Discussion:

- Sensitive information must never be read, displayed, discussed or used in public areas.
- Be careful about sensitive conversations in hotel conference rooms. Ensure everyone in the conference room has the proper security screening level, the need-to-know and that the door is closed.
- Do not use a wireless device to discuss sensitive matters. Use a wired telephone to discuss **Sensitive** matters.

1. IT Security Requirements

Production and storage of **Protected** data outside of the departmental premises must be done as per the following to ensure that the data remains secure at all times.

2.1 Electronic Storage

- Store **Protected** electronic documents on encrypted removable media (USB key) that use approved Government of Canada standards (FIPS 140-2 or above (ex: FIPS 140-3) certified removable media device, encrypted with AES 128, 192 or 256 bit algorithm and not be copied to a device which does not meet these requirements. <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>)
- Select strong passwords for your encrypted USB keys. The level of protection provided by such devices is directly related to the strength of the password chosen.

2.2 Electronic Possession, Transportation and Processing

When there is a requirement for the contractor to transport, process or electronically store departmental information, the contractor must ensure that the data remains secure at all times no matter what level of confidentiality the information is by adhering to the following requirements:

- Computing devices used to process data are equipped with up to date anti-virus software which is configured to automatically receive and install product updates;
- Computing devices used to process data must be equipped with up to date software and Operating System versions, and configured to automatically receive and install updates;
- Computing devices are protected by a firewall which can be a network perimeter firewall appliance or host based firewall application installed on the computer (note: a standard router only device is not considered a substitute to a firewall);
- The contractor has the means to securely dispose of electronic data in accordance with CSEC standards (refer to <https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006> Departmental data must be stored on a FIPS 140-2 or above certified removable media device that is encrypted with AES 128 bit algorithm or higher (refer to <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm> for a list of certified devices); and
- Portable storage devices must be labeled to indicate the highest classification or designation level of information stored on the device.



1.3 Electronic Transmission of Departmental Data

Electronic transmission of Protected data between the Contractor and the Department of Crown-Indigenous Relations and Northern Affairs Canada (CIRNAC) and Indigenous Services Canada (ISC) must be done as per the following approved method based on the level of sensitivity of the information. The contractor may use a combination of these transmission methods in order to share information with CIRNAC/ISC's personnel. The use of electronic transmission methods other than those listed below is prohibited.

Classification Level	CIRNAC/ISC Approved Transmission Methods	Requirements
Protected A	Email	<p>The Contractor can transmit Protected A Data to CIRNAC/ISC personnel via email as long as the following requirements are met:</p> <ul style="list-style-type: none"> • The e-mail account is not a publically accessible web-mail based service (ex: hotmail, yahoo mail, gmail etc); • Each user has their own corporate e-mail account which is protected with a username and password; and • Email server communication is protected with TLS encryption.
	Fax	<p>The Contractor can transmit Protected A Data to CIRNAC/ISC via fax as long as the following requirements are met:</p> <ul style="list-style-type: none"> • The sending fax machine is located on the contractor's premises; • The sender contacts the recipient to confirm fax number and advise recipient of incoming fax; • Recipient is present at the fax machine ready to receive fax; and • Sender obtains confirmation from sender of receipt.
	Wireless Communications	<p>If a wireless access point is installed on the contractor's premises, and devices processing CIRNAC/ISC data will be connected to this network, the wireless infrastructure must at a minimum include the following safeguards:</p> <ul style="list-style-type: none"> ▪ The administrator user name and password must be changed from their default values; ▪ The network name (SSID) has been changed from its default value; and ▪ WPA2 encryption with an AES algorithm enabled and the passphrase meets the following complexity requirements: <ul style="list-style-type: none"> • Must be 8 characters or longer; • Have at least one upper case character; • Have at least one lower case character; • Have at least one numeric character; and



		<ul style="list-style-type: none"> • Have at least one allowed special character
Protected B	Encrypted and Digitally Signed eMail	<p>The Contractor can transmit Protected B Data to CIRNAC/ISC personnel via email as long as the messages and/or attachments are encrypted and the following requirements are met:</p> <ul style="list-style-type: none"> • The e-mail account is not a publically accessible web-mail based service (ex: hotmail, yahoo mail, gmail etc); • Each user has their own corporate e-mail account which is protected with a username and password; • The contractor has an approved Public Key Infrastructure (PKI) certificate that is compatible with the Government of Canada (GoC) PKI services; and • Entrust software is installed on the contractor's PC/laptop and utilized to encrypt the email using the following settings: <ul style="list-style-type: none"> • One of the following encryption algorithms is used: <ul style="list-style-type: none"> ▪ 3DES-168 Bit or higher ▪ AES-128 Bit or higher • Digitally signed with one of the following algorithms: <ul style="list-style-type: none"> ▪ RSA (Rivest, Shamir, Adleman) ▪ DSA (Digital Signature Algorithm) ▪ ECDSA (Elliptic Curve Digital Signature Algorithm) • One of the following Hash functions is used in the generation of digital signatures: <ul style="list-style-type: none"> • SHA-224 • SHA-256 • SHA-384 • SHA-512
	Wireless Communications	<p>If a wireless access point is installed on the contractor's premises, and devices processing CIRNAC/ISC data will be connected to this network, the wireless infrastructure must at a minimum include the following safeguards:</p> <ul style="list-style-type: none"> ▪ The administrator user name and password must be changed from their default values; ▪ The network name (SSID) has been changed from its default value; and ▪ WPA2 encryption with an AES algorithm enabled WPA2 encryption with an AES algorithm enabled and the passphrase meets the following complexity requirements: <ul style="list-style-type: none"> • Must be 12 characters or longer; • Have at least one upper case character;



		<ul style="list-style-type: none"> • Have at least one lower case character; • Have at least one numeric character; and • Have at least one allowed special character
	CIRNAC/ISC Secure File Exchange Service	<p>The Contractor can transmit Protected B Data via CIRNAC/ISC's Secure File Exchange service as long as following requirements are met:</p> <ul style="list-style-type: none"> • A personally identifiable unique username and password is assigned to the user by CIRNAC/ISC; and • The contractor has read and agrees to abide to the Secure File Exchange Acceptable Use Policy (See annex 1 of security requirement agreement)
	CIRNAC/ISC Collaboration Service	<p>The Contractor can transmit Protected B Data via CIRNAC/ISC's Collaboration service as long as following requirements are met:</p> <ul style="list-style-type: none"> • A personally identifiable unique username and password is assigned to each user by CIRNAC/ISC.
	Fax	<p>The Contractor can transmit Protected B Data to CIRNAC/ISC via fax as long as the following requirements are met:</p> <ul style="list-style-type: none"> • • The sending fax machines is located on the contractor's premises; • The sender contacts the recipient to confirm fax number and advises recipient of incoming fax; • Recipient is present at the fax machine ready to receive fax; and • Sender obtains confirmation from sender of receipt.

3. Inspection

An authorized representative of the Government shall have the right to inspect, at reasonable intervals, the Contractor's methods and facilities for compliance with the Policy on Government Security requirements and this Agreement. The Contractor shall cooperate with the authorized representative and provide such information as the authorized representative may require in regard to any such inspections. Should the Government determine that the Contractor is not in compliance, it shall submit a written report to the Contractor advising of the deficiencies and follow-up on the deficiencies until they are rectified to the satisfaction of the department.

4. Security Costs

The Department shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder.



SECURITY AGREEMENT

I, _____ (Contractor) and authorized resources will fulfill the duties as contractor working under the contract _____, as set out below, to the best of our abilities.

1. Will abide by all of Indigenous Services Canada (ISC) security clauses and requirements included in this contract. Acknowledge receipt and understand these existing clauses and requirements, and promise to familiarize with any amendments to them, forthwith after receipt of such amendments.
2. Understand and agree that information received in the process of performing our duties in relation to this contract is subject to the Policy on Government Security and may be also subject to the Privacy Act, and will remain the property of CIRNAC/ISC. Without the prior written authorization of CIRNAC/ISC or of the person to whom the information relates, this information can only be viewed by myself and authorized resources and may only be used for the purposes of this contract on behalf of CIRNAC/ISC.
3. Agree to notify ISC authorities of any unauthorized access, disclosure or misuse of the sensitive information of which we become aware and will provide full details of the incident immediately noting the corrective action taken to prevent a recurrence of the incident.
4. Understand and agree that any additional resources authorized to perform work under this contract will also abide by all of ISC security clauses and requirements included in this contract.

I, the undersigned, UNDERSTAND, AGREE AND CONSENT TO COMPLY WITH THE ABOVE:

Contractor:

PRINT NAME: _____

SIGNATURE: _____

DATE: _____

CIRNAC/ISC Project Authority:

PRINT NAME: _____

SIGNATURE: _____

DATE: _____



ANNEX "D"

DEFINITIONS

- "Bug Fixes" means a temporary work-around, patch, or bypass to update the program code to correct errors or defects. "Downgrade" means that for Licensed Software that is capable of being 'downgraded' to a lower edition, Canada can opt to downgrade if the upgraded application is malfunctioning, running slow, and/or not operating properly.
- "Enhancement" also often referred to as an "interim release" means an interim release version of the Licensed Software, which is often documented by adding a further decimal and digit to the version or release number (e.g., V.X.X.2 would be the next enhancement after V.X.X.1).
- "Error" means any software instructions or statement contained in (or absent from) the Licensed Program that, by its presence or absence, prevents the Licensed Software from operating in accordance with the Specifications.
- "Extensions" means an update to the Licensed Software that extends the features, functionality or performance of the Licensed Software program code, regardless of whether the Contractor refers to it as an "extension".
- "New Release" means a system release, a version release, and interim release of the Licensed Software, regardless of whether the Contractor refers to it as a "new release".
- "Renames" means an upgrade to the Licensed Software where the product name is changed, but the new software product has similar features and functionality as the Licensed Software, regardless of whether the Contractor refers to it as a "rename".
- "Service Releases" means a release of the Software which is designed to operate on designated combinations of computer hardware and operating systems. A new System Release typically will be indicated by the addition of one (1) to the first digit of the release number (e.g. v.2.X.X would be the next System Release after v.1.X.X).
- "Software Patches" means an engineering fix to a problem that may be incorporated into a new release to update the Licensed Software in order to improve or correct errors or defects in the program code. "Software Publisher" means the entity who develops and markets the licensed software and owns the Intellectual Property.
- "Technical Support Organization" ('TSO') means those Contractor product specialists who make available technical support to Contractor's Clients who have contracted for and are current under Contractor's Maintenance Services.
- "Upgrades (major)" means an update to the Licensed Software to add, extend, enhance and/or improve the existing features, functionality and/or performance of the program code, which is documented by a version or build number change to the left of the first decimal (e.g., Product X Version 1.3 changes to Product 2.0 or Product X Version 1.1.5 changes to Product X Version 2.0.0), regardless of whether the Contractor refers to it as a "major upgrade".
- "Upgrades (minor)" means an update to the Licensed Software to add, extend, enhance and/or improve the existing features, functionality and/or performance of the program code, version or build number change to the right of the first decimal (e.g., Product X Version 1.0 changes to Product X Version 1.1 or Product X Version 1.0.0 changes to Product X Version 1.0.1), regardless of whether the Contractor refers to it as a "minor upgrade".
- "Version Release" means a release often involving a limited number of new or enhanced features or functionality or features and error corrections, which is often documented by adding a



second digit after the release number (e.g., V.X.2.X would be the next version release after V.X.1.X).