SERVICE AGREEMENT

MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT

DRAFT

BRITISH COLUMBIA Ministry of Children and Family Development	**MINISTRY SERVICE AGREEMENT:** **Agreement Name:**

HIS MAJESTY THE KING IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, represented by The Minister of Children and Family Development (the "Province", "we", "us", or "our" as applicable) at the following address:	AND ______________________________ (Legal Name) (the "Contractor", "you", or "your" as applicable) at the following address:
Fax Number: Email:	Fax Number: Email:

The term for the Service Agreement begins on: ____________________ (Day/Month/Year) and ends on ________________________ (Day/Month/Year)

THE PARTIES AGREE TO THE TERMS AND CONDITIONS OF THE SERVICE AGREEMENT LOCATED ON THE MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT'S WEBSITE, VERSION 1.4 DATED FEBRUARY 10, 2022, AND AGREE TO BE BOUND BY THE SCHEDULES LISTED BELOW AND ATTACHED TO THIS AGREEMENT:

SCHEDULE A	-	SERVICES
SCHEDULE B	-	PAYMENT
SCHEDULE C	-	APPROVED SUBCONTRACTOR(S)
SCHEDULE D	-	INSURANCE
SCHEDULE E	-	AUTHORIZED PERSON
SCHEDULE F	-	INFORMATION MANAGEMENT (RECORDS, PRIVACY AND SECURITY)
SCHEDULE G	-	ASSETS
SCHEDULE H	-	ADDITIONAL TERMS
SCHEDULE I	-	REPORTING REQUIREMENTS

(collectively, the
"Agreement")

SIGNED AND DELIVERED on the ______________day of ______________, ____________on behalf of the Province by its duly authorized representative Signature:	**SIGNED AND DELIVERED** on the ______________day of ______________, ____________ by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation) Signature: ______________________________
Print Name: ______________________________ Position:	Print Name: ______________________________ Position: ______________________________
Responsibility Centre:	Signature: ______________________________
	Print Name: ______________________________ Position: ______________________________

Contractor: By signing above you agree that you have read, understand, and agree to be bound by, the Terms and Conditions and the Schedules for the Service Agreement

DRAFT

SUMMARY

Term

Total Amount of Agreement (not including any applicable taxes)

Allocation by Programs and Services

Non-Program Services	
Sub-Total	
Total	

Allocation by Community

Communities Served	
Total	

Allocation by Business Area

Core Business Area	Business Area - Sub Business Area	
	Sub-Total	
	Total	

DRAFT

SCHEDULE A - SERVICES

SERVICE:			**Total Amount**
	Definitions		
	Project Code		
	Input		
	Output Indicators		**Quantity**
	Reporting Frequency		
	Core Business Area		
	Business Area		
	Communities Served		
		Recipient(s)	**Amount**

BUSINESS AREA OUTCOMES

DRAFT

SCHEDULE B – PAYMENT

Aggregate Maximum and Taxes

1.1 Subject to the provisions of the Agreement, we will pay you an amount not exceeding $ (not including any applicable taxes), in the aggregate, for providing the Services set out in Schedule A, during the term of this Agreement.

1.1 In addition, we will pay you any applicable taxes payable by the Province under law or agreement with the relevant taxation authority in relation to amounts payable under this schedule.

Payments

Monthly Recurring

2.1 We will pay you the fixed payment allocation of, on or about the 15th day of the month commencing on the day of , as provided in the following payment schedule:

Variable

2.1 We will pay you, to a maximum amount of invoiced to us as during the Term of the agreement.

2.2 In order to obtain payment of invoice, the Contractor must deliver to the Province a written statement of account in a form satisfactory to the Province containing:

1. the Contractor's legal name and address;
2. the date of the statement;
3. the Contractor's calculation of all fees claimed under this Agreement, including a declaration that the Services for which the Contractor claims fees have been completed;
4. a chronological listing, in reasonable detail, of any expenses claimed by the Contractor with receipts attached, if applicable, and, if the Contractor is claiming reimbursement of any GST or other applicable taxes paid or payable by the Contractor in relation to those expenses, a description of any credits, rebates, refunds or remissions the Contractor is entitled to from the relevant taxation authorities in relation to those taxes;
5. the Contractor's calculation of all applicable taxes payable by the Province in relation to the Services;
6. a description of this Agreement to which the statement relates;
7. a statement number for identification; and
8. any other billing information reasonably requested by the Province

SCHEDULE C – APPROVED SUBCONTRACTOR(S)

Subcontractors

1.1 The following persons, groups of persons, or organizations, are specified as Subcontractors under section 12 of the Service Agreement:

SCHEDULE D – INSURANCE

1. On behalf of the Contractor, the Province will purchase and maintain commercial general liability insurance in the amount of $2,000,000 inclusive per occurrence insuring against third party bodily injury, third party property damage, and personal and advertising injury, where any of them arise out of the performance of the Services by the Contractor and/or by approved subcontractors who have entered into a written agreement to perform the Services.

2. The Contractor is responsible for and will pay any deductible under the insurance policy.

3. The Province will obligate the managing broker to provide the Contractor with a Certificate of Insurance and a copy of the insurance policy wording.

4. The Province will take reasonable steps to ensure the coverage specified in section 1 is continuous for the duration of this Agreement. The Province will not be responsible for providing coverage in the event the insurance is cancelled or reduced by the insurer.

5. The Province does not represent or warrant that the insurance covers any and all losses. The Contractor is responsible for ascertaining the exact nature and extent of coverage of the insurance policy as well as the terms and conditions of the insurance policy. No term or condition of this Agreement amends, extends or alters the coverage afforded by the insurance policy.

6. Where the Contractor uses a vehicle to perform the Services the Contractor shall maintain Automobile Liability insurance on all vehicles owned, operated or licensed by the Contractor in an amount not less than $2,000,000 per occurrence, and where applicable the Contractor may show evidence of this insurance using an ICBC Confirmation of Insurance Coverage (APV-47) form.

The below language will be used instead of the above if the Contractor is not eligible for the Social Services Group Liability Program (SSGLP)

---

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Province:

(a) Commercial General Liability in an amount not less than $2,000,000.00 inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must

(i) include the Province as an additional insured,

(ii) be endorsed to provide the Province with 30 days advance written notice of cancellation or material change, and

(iii) include a cross liability clause.

(b) Where the contractor uses a vehicle to perform the services as described in Schedule A the Contractor shall maintain Automobile Liability insurance on all vehicles owned, operated or licensed by the Contractor in an amount not less than $2,000,000 per occurrence, and where applicable the Contractor Agreement No: 8 of 18 DRAFT may show evidence of this insurance using an ICBC Confirmation of Insurance Coverage (APV-47) form.

2. All insurance described in section 1 of this Schedule must:

(a) be primary; and

(b) not require the sharing of any loss by any insurer of the Province.

3. The Contractor must provide the Province with evidence of all required insurance as follows:

(a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Province evidence of all required insurance in the form of a completed Province of British Columbia Certificate of Insurance;

(b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Province within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and

(c) despite paragraph (a) or (b) above, if requested by the Province at any time, the Contractor must provide to the Province certified copies of the required insurance policies. 4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

DRAFT

SCHEDULE E – AUTHORIZED PERSONS

Authorized Persons

1.1 The Contractor designates any of the following persons, (identified by name and/or position) to act for you in relation to this Service Agreement:

Name	Position	Email Address

1.2 The Ministry designates any of the following persons (identify by name and/or position) to act for us in relation to this Service Agreement:

Name	Position	Email Address

Conflict Resolution Officials

1.1 The designated "Officials" of the parties for the purposes of the Conflict Resolution Protocol are:

	Province	Contractor
Stage One:		
Stage Two:		
Stage Three:		

SCHEDULE F – INFORMATION MANAGEMENT (RECORDS PRIVACY AND SECURITY)

Purpose

The purpose of this Schedule is to:

(a) enable the Province to comply with the Province’s obligations with respect to:

(i) creation, maintenance, retention and final disposition of the Province’s Records, and

(ii) protection of Personal Information collected or created under this Agreement and pursuant to FOIPPA.

(a) ensure that, as a service provider, the Contractor is aware of, and complies with, the Contractor’s information management and protection (records, privacy and security) obligations with respect to:

(i) the Province’s Records, and

(ii) the Protected Information collected or created under this Agreement.

Applicability

This Schedule applies to the management of the Province’s Records and to the management of Protected Information contained in the Province’s Records.

The Contractor must manage the Province’s Records in accordance with this Schedule and in accordance with MCFD Contractor’s Information Management Guidelines, which provide directions and standards to assist the Contractor in complying with this Schedule.

Definitions

2. In this Schedule:

(a) “**access**” means disclosure by the provision of access. For clarity, this includes the ability or opportunity of a person to view, study, or obtain a copy of records;

(b) “**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

(c) “**control”** (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use and disclosure**;**

(d) **“custody” (**of a record) means having physical possession of a record, regardless of the format (e.g. paper or electronic);

(e) “**Device**” means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement;

(f) “**Facilities**” means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information;

(g) “***FOIPPA***” means the *Freedom of Information and Protection of Privacy Act* (British Columbia);

(h) “**Least Privilege**” means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use;

(i) "**Need-to-Know**" means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office;

(j) "**Personal Information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Province or the Contractor dealing with the same subject matter as the Agreement, but excluding any information that, if this Schedule did not apply to it, would not be under the control of a public body within the meaning of FOIPPA;

(k) "**Personnel**" means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor's obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual;

(l) "**Policies**" means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines);

(m) "**Privacy Training**" means the Province's online privacy and information sharing training course;

(n) "**Protected Information**" means any and all:

(i) "personal information" as defined in this Schedule;

(i) information and records of information the Contractor is required to treat as confidential under this Agreement; and

(ii) records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as "Protected Information" under this Agreement;

(o) "**Security Event Logs**" means any logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls);

(p) "**Systems**" means any systems, subsystems, equipment, infrastructure, networks, management networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement;

(q) "**Tenancy**" means those components of the Systems that:

(i) directly access and store Protected Information,

(i) relate to Protected Information or the Province's tenancy activities, or

(ii) are customer facing and managed by the Province in its use of the Services; and

(r) "**Tenancy Security Event Logs**" means Security Event Logs that relate to Tenancy, including:

(i) log-on/log-off information about Province user activities, and

(i) application logs, web server log, file server logs, database logs of applications, web servers, file servers or database servers or any other logs that directly store, access or contain Protected Information.

RECORDS MANAGEMENT

Records Retention and Disposition

3. The Contractor must return the Province's Records regardless of format to the Province within the following time frames:

   (a) within 30 calendar days of expiry or termination of the Agreement;

   (b) within 7 calendar days of the Contractor receiving a request for return from the Province;

   (c) when closed records volume is identified by the Contractor as warranting the transfer and the Province has provided written approval; or

   (d) immediately when a Contractor advises the Province that they are no longer providing services or when the Province is concerned about the management of the Province's Records following a breach of security or privacy, including an unauthorized disclosure.

PRIVACY PROTECTION

Collection of Personal Information

4. The Contractor may only collect or create Personal Information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect Personal Information directly from the individual the Personal Information is about.

6. Except as otherwise permitted by FOIPPA, the Contractor must tell an individual from whom the Contractor collects Personal Information:

   (a) the purpose for collecting it,

   (b) the legal authority for collecting it, and

   (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Contractor's collection of Personal Information.

Accuracy of Personal Information

7. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any Personal Information to be used by the Contractor or the Province to make a decision that directly affects the individual the Personal Information is about.

Requests for access to Personal Information

8. If the Contractor receives a request for access to Personal Information from a person other than the Province, the Contractor must promptly advise the person to make the request to Information Access Operations with the Ministry of Citizens' Services or successor.

Correction of Personal Information

9. Within 5 business days of receiving a written direction from the Province to correct or annotate any Personal Information, the Contractor must correct or annotate the information in accordance with the direction.

10. When issuing a written direction under section 9 of this Schedule, the Province must advise the Contractor of the date the correction request to which the direction relates was received by the Province in order that the Contractor may comply with section 11 of this Schedule.

11. Within 5 business days of correcting or annotating any Personal Information under section 9 of this Schedule, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Contractor disclosed the information being corrected or annotated.

12. If the Contractor receives a request for correction of Personal Information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and provide the Provincial official's name or title and contact information to the person making the request.

Protection of Personal Information

13. The Contractor must protect Personal Information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any security arrangements expressly set out in the this Schedule.

Storage and access to Personal Information

14. Unless the Province otherwise directs in writing, the Contractor must not store Personal Information outside Canada or permit access to the Personal Information from outside Canada.

Retention of Personal Information

15. Unless the Agreement otherwise specifies, the Contractor must retain Personal Information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of Personal Information

16. Unless the Province otherwise directs in writing, the Contractor may only use Personal Information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of Personal Information

17. Unless the Province otherwise directs in writing, the Contractor may only disclose Personal Information inside Canada to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

18. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not disclose Personal Information outside Canada.

PERSONNEL

Confidentiality agreements

19. The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under this Agreement.

Personnel security screening

20. The Contractor may only permit individual Personnel to have access to any Protected Information or other asset of the Province (including to any system, network or device the Province makes available to the Contractor) in relation to this Agreement, if, after:

(a) verifying their identity and relevant education, professional qualifications and employment history;

(b) completing a criminal record check that is updated at least every five years;

(c) requiring Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law;

(d) performing any additional screening this Agreement or applicable law may require; and

(e) performing any additional background checks the Contractor considers appropriate,

the Contractor is satisfied that the individual does not constitute an unreasonable security risk.

21. If any criminal record check or proactive disclosure reveals a prior criminal offence or pending criminal matter, the Contractor must make a reasonable determination of whether the applicable person constitutes an unreasonable security risk, taking into consideration the duties of the individual and the type and sensitivity of information to which the individual may be exposed.

22. If the Contractor is an individual, the Province may subject the Contractor to the screening requirements in this Schedule.

Personnel information security training

23. Unless otherwise specified in this Agreement, the Contractor must ensure all Personnel complete any relevant information security training, at the Contractor's expense, before they provide any Services, or receive or are given access to any Protected Information or any system, device or secure facility of the Province, and thereafter at least annually.

Security contact

24. If not set out elsewhere in this Agreement, the Contractor (but not a Subcontractor) must provide in writing to the Province the contact information for the individual who will coordinate compliance by the Contractor and all Subcontractors and act as a direct contact for the Province on matters relating to this Schedule.

Supply chain

25. The Contractor must ensure that the security requirements of those in its upstream and downstream supply chain are documented, followed, reviewed, and updated on an ongoing basis as applicable to this Agreement.

GENERAL POLICIES AND PRACTICES

Privacy Training

26. The Ministry will pay the direct costs of the Privacy Training, the Contractor, must ensure that:

(a) all employees, agents, volunteers and Subcontractors who collect, create, or access Protected Information, complete Privacy Training;

(b) all employees, agents, volunteers and Subcontractors engaged subsequent to the signing of this Agreement who will collect, create or access Protected Information have completed the provincially required Privacy Training prior to accessing Protected Information; and,

(c) a log is maintained with the names of all employees, agents, volunteers and Subcontractors who collect, create, or access Protected Information which indicates the status of their completion of the Privacy Training including date of completion. The Contractor must make this log available to the Province upon request.

Compliance, Audit and Review

27. The Contractor must, in relation to the Province's Records, comply with:

(a) the requirements of FOIPPA applicable to the Contractor as a service provider, including any applicable order of the commissioner under FOIPPA, and

(b) any direction given by the Province under this Schedule.

28. The Contractor acknowledges that it is familiar with the requirements of FOIPPA governing Personal Information that are applicable to it as a service provider.

Inspection of personal information

29. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect, and at the Province's discretion, copy, any of the Province's Records, or any of the Contractor's information management policies or practices or Records relevant to the Contractor's management of the Province's Records or the Contractor's compliance with this Schedule. The Contractor must permit and provide reasonable assistance to any such inspection.

30. If the Province conducts a review of a matter described in section 90 of this Schedule (whether or not the matter came to the attention of the Province as a result of a notification under section 90 of this Schedule), the Contractor must, on the request of the Province, participate in the review to the extent that it is reasonably practicable for the Contractor to do so.

Information security Policy

31. The Contractor must have an information security Policy that is:

(a) based on recognized industry standards; and

(b) reviewed and updated at least every three years.

Compliance and Standard for Security Controls

32. Unless this Agreement otherwise specifies, the Contractor must apply controls and security management practices to manage or operate Protected Information and Systems, Devices, and Facilities that are compliant with or equivalent to the following Province's Policies accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures:

(a) "Information Security Policy";

(b) government wide IM/IT Standards; and

(c) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

Contractor security risk assessments

33. The Contractor must undertake a security threat and risk assessment against an industry security standard before placing any new or materially changed Systems or services into production.

Change control and management

34. The Contractor must:

    (a) implement and maintain change control processes for Facilities, Systems and Devices in line with applicable security best practices to reduce security-related risks with respect to implemented significant changes; and

    (b) ensure that adequate testing of any change is completed before the change is put into production.

Backups and restores

35. The Contractor must ensure that:

    (a) it has a backup Policy that is followed and is reviewed, updated and tested at least annually;

    (b) backups are taken and tested in accordance with the Contractor's backup Policy, but in any event at least annually; and

    (c) frequency and completeness of backups is based on reasonable industry practice.

Business continuity plan and disaster recovery plan

36. The Contractor must ensure that it has a documented business continuity plan and a disaster recovery plan that is reviewed at least annually.

37. The Contractor must ensure that Facilities and Systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those Facilities and Systems being unavailable when required to provide the Services.

Security Incident Response and Management

38. The Contractor must ensure that it has a security incident management Policy and response plan that is reviewed at least annually.

PROTECTED INFORMATION AND DATA SECURITY

Encryption

39. The Contractor must ensure that:

    (a) encryption of data at rest is implemented and is maintained in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, for all Protected Information stored on Systems and Devices; and

    (b) encryption end-to-end is implemented for all Protected Information in transit.

No storage on unencrypted portable media

40. The Contractor must ensure that no Protected Information is stored on portable media for transport outside of the Facilities or Systems without both the prior written approval of the Province and ensuring that the portable media and the Protected Information are encrypted.

Encryption standard

41. For sections 39 and 40, encryption must comply with the Province's "Cryptographic Standards for Information Protection" accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures.

Isolation controls and logical isolation of data

42. The Contractor must implement and maintain the logical isolation of Protected Information, in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

ACCESS AND AUTHENTICATION

User Identifiers

43. The Contractor must assign and ensure that user identifiers are unique and personal for log in to Systems and Devices.

Access

44. The Contractor must implement, follow, and regularly review and update, access control Policies that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts for Facilities, Systems and Devices within the Contractor's control.

45. The Contactor must ensure that all access to Protected Information and to Facilities, Systems and Devices is based Least Privilege and Need-to-Know" based on role and responsibilities. The Contractor must identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse.

46. The Contractor must verify an individual's identity before assigning the individual a unique identifier that would give them access to Facilities, Systems or Devices.

47. The Contractor must implement a formal user registration process for Personnel that includes:

    (a) verification of access levels;

    (a) creating and maintaining records of access privileges;

    (b) audit processes; and

    (c) actions to ensure access is not given before approval is granted by the Contractor.

48. The Contractor must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts.

49. The Contractor must implement a monitoring process to oversee, manage and review Personnel access rights and roles at regular intervals.

50. The Contractor must ensure that all Systems and Devices:

    (a) are configured in alignment with industry standards;

    (b) enforce a limit of consecutive invalid logon attempts by a user during a predetermined time period;

    (c) automatically lock the applicable account and Systems after failed logon failures;

(d) limit the number of concurrent sessions;

(e) prevent further access to Systems by initiating a session lock; and

(f) provide the capability of disconnecting or disabling remote access to the Systems.

Authentication

51. The Contractor must use or require complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that are encrypted (not displayed) when entered, biometric accesses, keys, smart cards, other logical or access controls, or combinations of them, to control access to Protected Information and to Systems and Devices.

52. The Contractor must ensure that Systems for password-based authentication:

(a) enforce minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;

(b) change authentication passwords regularly at predetermined intervals, but at a minimum semi-annually;

(c) store and transmit only encrypted representations of passwords;

(d) enforce password minimum and maximum lifetime restrictions;

(e) prohibit password reuse;

(f) prevent reuse of identifiers; and

(g) disable the identifier after ninety days of inactivity.

Highly sensitive Protected Information

53. If this Agreement or the Province under this Agreement indicates that any Protected Information is highly sensitive, the Contractor must also ensure that Systems enforce with respect to that Protected Information:

(a) two-factor authentication for access;

(b) enhanced logging that logs all accesses;

(c) request based access; and

(d) no standing access rights.

SECURITY EVENT LOGS

Log generation, log retention and monitoring

54. The Contractor must ensure that logging of Security Event Logs is enabled on all applicable Systems components

55. The Contractor must retain Security Event Logs for the Systems online for a minimum of 90 days and either online or off-line for an additional period of time adequate to enable the Contractor to conduct effective security investigations into suspected or actual security incidents.

56. The Contractor must retain Tenancy Security Event Logs online for a minimum of 90 days and either:

(a) such additional period of time as the Province may instruct; or

(b) ensure that the Tenancy offers the technical capability for the Province to retain the Tenancy Security Event Logs,

to enable the Province to comply with an information schedule approved under the *Information Management Act* or other retention period required by law.

57. Upon the Province's request, the Contractor must ensure that the Tenancy offers the technical capability for the Province to enable or configure the forwarding, extraction, backup of Tenancy Security Event Logs from the Tenancy to the Province's security information and event management system or to an external log storage and retention system.

58. The Contractor must review Security Event Logs regularly to detect potential security incidents, using automated tools or equivalent processes for the monitoring, review, correlating and alerting of Security Event Logs.

PROVINCE PROPERTY

Access to Province facilities, systems or networks

59. If the Province makes available any facilities, systems, networks or devices for use of the Contractor in relation to this Agreement, the Contractor must comply with, and permit access on its behalf only by those authorized Personnel who have been instructed to comply with, the Province's Policies then applicable to their acceptable use, access and protection accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures, including:

(a) "Appropriate Use Policy" (as also referenced in chapter 12 of the Province's "Core Policy and Procedures Manual");

(b) "Information Security Policy";

(c) government wide IM/IT Standards; and

(d) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

60. The Province has the rights to:

(a) not make any particular Province facility, system, network or device available before the Contractor or individual Personnel or both agree to a form of agreement acceptable to the Province on acceptable use, protection of, and access to, such facility, system, network or device, or at all;

(a) not permit connection to any particular Province system or network until satisfied with the controls applied and the security status of the Device to be connected;

(b) keep facilities access logs and Security Event Logs, and to otherwise monitor and analyze use of Province facilities, systems and networks to verify compliance, investigate suspected or actual breaches or information incidents and protect the Province's assets, including records, in compliance with applicable laws, including the *Freedom of Information and Protection of Privacy Act* and *Information Management Act*, and the Province's Policies; and

(c) limit or revoke access to any Province systems, facility or device at its discretion.

Application development

61. If the Services include software development, the Contractor must ensure that the applications and programming interfaces are developed according to industry standards and Province's Policies applicable to application development standards. The Contractor must use secure application development practices for the development of the software.

FACILITIES, SYSTEMS, DATABASE AND DEVICE SECURITY

Physical security

62. The Contractor must ensure that adequate physical controls and processes are implemented to ensure that only authorized persons have physical access to the Facilities and Systems.

63. The Contractor must develop, document, and disseminate a physical and environmental protection Policy that it reviews at least annually.

64. The Contractor must review physical access logs at least once monthly.

65. The Contractor must ensure that physical security of any Systems or Facilities being used or capable of being used to house Protected Information meets a standard as would be reasonably expected to provide adequate protection based on the value of the data being protected and the environment in which the Systems or Facilities are located. At a minimum, this should include:

(a) hardening of the perimeter of the Facilities;

(b) physical separation of public and restricted spaces;

(c) Intrusion Alarm System (IAS) partitioned to ensure areas containing Protected Information are protected at all times;

(d) Access Control Systems (ACS) and/or Key Management processes; and

(e) visitor and identity management processes – including access logs and identification badges.

Separation of production from test environments

66. The Contractor must not use any production data in any development, test or training environments used for the Services without the Province's prior written consent. If the Province gives such consent, the production data must, at minimum, be obfuscated (for example, by using data masking functionality).

67. The Contractor must keep its development, test and training environments separate from its production environments used for the Services at all times, even in case of failure.

Systems (including servers) hardening

68. The Contractor must:

(a) harden all Systems against attack and misuse, using appropriate security best practices for the hardening of the specific deployed platform, before placing those Systems into production;

(b) ensure that all unsecured and unneeded ports, services, applications, protocols and network communicating applications are uninstalled or disabled on all Systems;

(c) applying Least Privilege, ensure that the Contractor only configures and makes operational ports, services, applications, protocols and network communicating applications based on the functional requirements of the respective Systems;

(d) ensure that default passwords and shared accounts are not used for any Systems; and

(e) in relation to Systems, implement server hardening using configuration security best practices (for example, Center for Internet Security, Inc. (CIS) Benchmarks or equivalent) for any server operating systems, server virtualization, server middleware (for example, web servers and database servers) and application servers.

Perimeter controls (firewall and intrusion prevention system) and network security

69. The Contractor must:

(a) implement stateful packet inspection firewalls to control traffic flow to and from Systems and Tenancy at all times, and configure the stateful packet inspection firewalls applying security best practices and Least Privilege;

(b) implement an intrusion prevention System to control and filter traffic flow leaving and entering Systems and Tenancy at all times, and configure the intrusion prevention System applying security best practices; and

(c) implement a secure network perimeter and network segmentation for Systems, with ingress and egress points that are known and controlled.

Application firewall

70. The Contractor must implement application layer firewalls on Systems:

(a) at such level of protection as the Province may instruct ; and

(b) to detect and mitigate application attacks (for example, brute force, OWASP Top 10, SQL injection, cross site scripting).

Management network

71. The Contractor must ensure that for any Systems:

(a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;

(b) the management network is internally segmented, with each server's dedicated network interface on its own segmented network and that interfaces on the management network do not have visibility to each other; and

(c) all access to the management network is strictly controlled and exclusively enforced though a secure access gateway, bastion host or equivalent.

Remote management and secure access gateway

72. The Contractor must perform any remote management of Systems or Devices in a secure manner, using encrypted communication channels and adequate access controls.

Database security

73. The Contractor must ensure that for any Systems:

(a) database maintenance utilities that bypass controls are restricted and monitored;

(b) there is a formal approval process in place for handling requests for disclosure of database contents or for database access, including steps to evaluate privacy impacts and security risks of such requests; and

(c) methods to check and maintain the integrity of the data are implemented (for example, consistency checks and checksums).

74. For database security, the Contractor must implement logical isolation and encryption of Protected Information.

Device security and antivirus scanning

75. The Contractor must ensure all Devices:

    (a) have antivirus and malware protection as appropriate for the particular Device active at all times;

    (b) are configured to perform antivirus scans at least once per week;

    (c) have host based firewall configured, enabled and active at all times; and

    (d) have all patches and appropriate security updates installed for the operating system and all installed software.

VULNERABILITY PREVENTION, SCANNING AND MANAGEMENT

Proactive management

76. The Contractor must:

    (a) obtain information in a timely basis about technical vulnerabilities relating to Systems and Devices; and

    (b) implement processes to stay current with security threats.

Patching

77. The Contractor must patch all Systems regularly in line with security best practices and ensure that current software, operating systems and application patching levels are maintained.

78. The Contractor must ensure that all Systems have all patches installed on a regular schedule, within the time frame recommended by the manufacturer unless the Province otherwise consents in writing.

79. The Contractor must ensure that vulnerabilities are remedied and patches installed on an accelerated basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities, the Contractor must implement appropriate mitigation measures promptly on notification of the zero-day vulnerability. The Contractor must remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls.

80. The Contractor must patch high vulnerabilities within 30 days or less of discovery and patch medium vulnerabilities within 90 days or less of discovery.

Vulnerability Scanning

81. The Contractor must ensure that a vulnerability scan is completed on components of all Systems:

    (a) with any identified vulnerabilities remedied, before being placed into production; and

    (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Web application vulnerability scanning

82. The Contractor must ensure that a vulnerability scan is completed on any web applications used for Tenancy or in any other Systems:

    (a) and on any major changes to such web applications, with any identified vulnerabilities remedied, before being placed into production; and

(b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Antivirus and malware scanning

83. The Contractor must ensure that all Systems servers:

(a) have antivirus and malware protection configured, active and enabled at all times;

(b) have antivirus and malware definitions updated at least once a day; and

(c) are configured to undergo a full anti-virus scan for latent infections (to detect infections missed by the real-time agent) at least once a week.

DISPOSALS

Asset disposal

84. The Contractor must ensure that all disposals of assets used in providing or relating to the Services are done in a secure manner that ensures that Protected Information cannot be recovered.

Asset management

85. The Contractor must have asset management and disposal Policies that are followed, and reviewed and updated regularly in line with security best practices, and that address hardware, software and other critical business assets.

86. The Contractor must keep an asset management inventory that includes the name of the System, location, purpose, owner, and criticality, with assets added to inventory on commission and removed on decommission.

Information destruction and disposal

87. Unless this Agreement otherwise specifies, the Contractor must retain all records containing Protected Information in the Contractor's possession until instructed by the Province in writing to dispose or deliver them as instructed.

88. The Contractor must securely erase:

(a) records that contain Protected Information and Tenancy Security Event Logs when instructed in writing by the Province; and

(b) any backup, transitory and extra copies of records that contain Protected Information or Tenancy Security Event Logs when no longer needed in relation to this Agreement.

89. The Contractor must ensure that Protected Information and Tenancy Security Event Logs on magnetic media are securely wiped by overwriting using procedures and adequate media wiping solutions, degaussing, or other method in line with security best practices for disposal of media.

NOTICES, INCIDENTS AND INVESTIGATIONS

Notice of demands for disclosure

90. In addition to any obligation the Contractor may have to notify or assist the Province under applicable law, including as contemplated by section 30.2 of the Act, or this Agreement, if the Contractor is or has been required (including, but not limited to, under an enactment or a subpoena, warrant, order, demand or other request from a court, government agency or other legal authority) to produce, provide access to or otherwise disclose any Protected Information, the Contractor must, , immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

E-discovery and legal holds

91. The Contractor must fully co-operate with the Province to enable the Province to comply with e-discovery and legal hold obligations.

Incidents

92. In addition to any obligation the Contractor may have under applicable law, including the *Freedom of Information and Protection of Privacy Act,* or this Agreement, if, during or after the Term, the Contractor discovers a suspected or actual unwanted or unexpected event or series of events that threaten the privacy or security of Protected Information (including its unauthorized access, collection, use, disclosure, alteration, storage or disposal) or Tenancy, whether accidental or deliberate, the Contractor must:

(a) immediately report the particulars of such incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable (if unable to contact the Province's contract manager or other designated contact for this Agreement, the Contractor must follow the procedure for reporting and managing information incidents on the Province's website at https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents; and

(b) make every reasonable effort to recover the records containing Protected Information and contain and remediate such incident, following such reasonable instructions as the Province may give.

Investigations support and security investigations

93. The Contractor must:

(a) conduct security investigations in the case of incidents (including any security breach or compromise) affecting Devices, Facilities, Systems, Tenancy or Protected Information, collecting evidence, undertaking forensic activities and taking such other actions as needed;

(b) provide the Province with any related investigation reports, which the Contractor may sanitize first;

(c) upon the Province's request, provide the Province with any logs relating to such investigation reports as validation/confirmation of such investigation, which the Contractor may sanitize first; and

(d) maintain a chain of custody in all such security investigations it undertakes.

94. Upon the Province's request, the Contractor must:

(a) provide investigative support to the Province to enable the Province to conduct its own security investigations into incidents (including security breaches or compromises) affecting the Tenancy or Protected Information;

(b) provide the Province with timely access via an on-line, real-time GUI (Graphic User Interface) facility to any Tenancy Security Event Logs and to other Security Event Logs for Systems (the latter of which the Contractor may sanitize first to mask or remove, for example, data pertaining to the Contractor's customers) to assist the Province in conducting the Province's security investigations, or in case of technical limitations, other method acceptable to the Province (for example, on-site visits to enable direct access to those Security Event Logs).

95. The Contractor must work with and support the Province if the Province needs assistance in legal proceedings in relation to security investigations related to Protected Information or Tenancy.

Province Security Threat and Risk Assessment (“STRA”) support

96. The Contractor must, via its technical and security resources, support the Province in completing a STRA for the Services and to otherwise assess the risks associated with the Services, including by providing all information and documentation (for example, architecture diagrams, service architecture, controls architecture and technical information), which the Contractor may sanitize first and that the Province may reasonably require for such purpose.

Notification of changes

97. The Contractor must notify the Province of any changes to its security Policies, management practices and security controls described in this Agreement that may potentially negatively impact the security of Tenancy, Protected Information, or those Systems providing the Services.

Compliance verification

98. Upon the Province’s request, the Contractor must provide, at no additional cost, the following security reports to the Province at least every six months during the Term:
    (a) vulnerability scan reports of those Systems providing the Services; and
    (b) patch status reports for those Systems providing the Services.

99. In addition to any other rights of inspection the Province may have under this Agreement or under statute, the Province has the rights, at any reasonable time and on reasonable notice to the Contractor, to:

    (a) request the Contractor to verify compliance with this Schedule and to keep security controls documentation or records to support compliance; and
    (b) enter on the Contractor premises and Facilities to inspect and to validate the Contractor’s compliance with the security obligations under this Agreement

100. The Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province’s rights under this section. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require the Contractor, at the Contractor’s expense, to develop and implement a corrective action plan within a reasonable time.

Notice of non-compliance

101. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

MISCELLANEOUS

Interpretation

102. In this Schedule, unless otherwise specified, references to sections by number are to sections of this Schedule.

103. Any reference to the “Contractor” in this Schedule includes any Subcontractor, agent, or volunteer retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such Subcontractors, agents, and volunteers comply with this Schedule.

104. If a direction or provision of the Agreement or any Schedule conflicts with a requirement of FOIPPA or an applicable order of the commissioner under FOIPPA, the conflicting provision of the Agreement or Schedule will be inoperative to the extent of the conflict.

105. If there is a conflict between a documented process required by this Schedule to be created or maintained by the Contractor and this Schedule, the provision of this Schedule will prevail to the extent of the conflict.

106. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 107 of this Schedule, the law of any jurisdiction outside Canada.

107. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with FOIPPA.

108. Any reference to a specified Policy refers to it as may be revised or replaced from time to time.

Referenced documents

109. Policies and other documents of the Province referenced in this Schedule may be updated or replaced by the Province from time to time without notice, and if not found at the hyperlink or URL provided or via the Province's main website at http://www.gov.bc.ca, be obtained from the Province's contact for this Agreement.

Survival

110. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

SCHEDULE F – Appendix F1 – Security screening requirements

The personnel security screening requirements set out in this Appendix F1 are for the purpose of assisting the Contractor to determine whether or not a Services Worker constitutes an unreasonable security risk.

Verification of name, date of birth and address

1. The Contractor must verify the name, date of birth and current address of a Services Worker by viewing at least one piece of "primary identification" of the Services Worker and at least one piece of "secondary identification" of the Services Worker, as described in the table following this section. The Contractor must record which primary and secondary identification the Contractor examined, but must not copy or record any information from these identifications. For a Services Worker from another province or jurisdiction, reasonably equivalent identification documents are acceptable.

Primary Identification	Secondary Identification
Issued by ICBC: • B.C. driver's licence or learner's licence (must have photo) • B.C. Identification (BCID) card **Issued by provincial or territorial government:** • Canadian birth certificate **Issued by Government of Canada:** • Canadian Citizenship Card • Permanent Resident Card • Canadian Record of Landing/Canadian Immigration Identification Record	• School ID card (student card) • Bank card (only if holder's name is on card) • Credit card (only if holder's name is on card) • Passport • Foreign birth certificate (a baptismal certificate is not acceptable) • Canadian or U.S. driver's licence • Naturalization certificate • Canadian Forces identification • Police identification • Foreign Affairs Canada or consular identification • Vehicle registration (only if owner's signature is shown) • Picture employee ID card • Firearms Acquisition Certificate • Social Insurance Card (only if has signature strip) • B.C. CareCard • Native Status Card • Parole Certificate ID • Correctional Service Conditional Release Card

*It is not necessary that each piece of identification viewed by the Contractor contains the name, date of birth and current address of the Services Worker. It is sufficient that, in combination, the identification viewed contains that information.

Verification of education and professional qualifications

2. The Contractor must verify, by reasonable means, any relevant education and professional qualifications of a Services Worker, obtain or create, as applicable, Records of all such verifications, and retain a copy of those Records.

Verification of employment history and reference checks

3. The Contractor must verify, by reasonable means, any relevant employment history of a Services Worker, which will generally consist of the Contractor requesting that a Services Worker provide employment references and the Contractor contacting those references. If a Services Worker has no relevant employment history, the Contractor must seek to verify the character or other relevant personal characteristics of the Services Worker by requesting the Services Worker to provide one or more personal references and contacting those references. The Contractor must obtain or create, as applicable, Records of all such verifications and retain a copy of those Records.

Security interview

4. The Contractor must allow the Province to conduct a security-focused interview with a Services Worker if the Province identifies a reasonable security concern and notifies the Contractor it wishes to do so.

DRAFT

SCHEDULE G – ASSETS

Property

1.1 The following property to be acquired by you with funds to be paid by us under this Service Agreement is specified in this Service Agreement as property to be owned by us:

1.2 The following property provided by us to you or a subcontractor for the purposes of this Service Agreement is to be owned by you or subcontractor as indicated:

SCHEDULE H – ADDITIONAL TERMS

DRAFT

SCHEDULE I – REPORTING REQUIREMENTS

Delivery of Reports

1.1 Any report submitted to the Province by the Contractor pursuant to this Schedule must be submitted by a date and in a format to be determined by the Province in its sole discretion.

Service Delivery Reports

1.2 In addition to any other reporting obligations that the Contractor may have under this Agreement, the Province may request at any time and the Contractor must respond with reports relating to the delivery of Services under the Agreement. Such reports may include, but may not be limited to, information about the Contractor's progress delivering the Services, its work done, key performance indicators, timelines, and more.

Financial Reports

1.3 In addition to the financial statements required by and referred to in this Agreement's provisions concerning Audits and Services Evaluations (as described in the Agreement), any financial reports further required under section 1.4 of this Schedule must include information reporting on, at a minimum, the outputs, deliverables, and Output Indicators described in Schedule A.

1.4 The following additional financial reports are required:

Additional Reports

1.5 The Province may at any time submit to the Contractor a request for additional reports.

1.6 If the Province submits to the Contractor a request for additional reports, then the Contractor must provide to the Province any such reports that the Province, in its sole discretion, determines that it requires to support its goals; for example, for supporting contracted sector wage increases. These reports may include but need not be limited to the following in relation to the Contractor's employees:

a) Position titles;
b) Job classifications (e.g. grid, level, steps, etc.);
c) Wages' rates and benefits; and

Any other data, as required in the Province's sole discretion.