BC Services Card Authentication Service
Service Agreement

BETWEEN

Her Majesty the Queen in Right of the Province of British Columbia
as Represented by the
Minister of Technology, Innovation and Citizens' Services (MTICS),
Provincial Identity Information Management Program (IDIM)

AND

Her Majesty the Queen as Represented by the Minister of <<Name>>
<<Program Area>>
(BCSC Client)

Hereinafter collectively referred to as the Parties

{Page left intentionally blank}

TABLE OF CONTENTS

1. PURPOSE

MTICS manages and provides corporate authentication services on behalf of the Province through IDIM. The BCSC Client wishes to access and use IDIM's BC Services Card (BCSC) Authentication Service to deliver its service: <<Service Name>> <<and description >>.

This Service Agreement (the Agreement) sets out the terms and conditions under which the BCSC Client is authorized to access and use IDIM's BCSC Authentication Service to deliver its <<Service Name>> to End Users. It also defines the roles and responsibilities of the Parties as they relate to the use of the BCSC Authentication Service.

Both Parties will execute this Agreement prior to the technical integration of the Parties' systems being deployed into the production environment.

2. DEFINITIONS

In this Agreement:

Agreement Administrator – a senior representative authorized on behalf of each Party to sign this Agreement. They are responsible for ensuring that due diligence to comply with the terms, conditions, rights and obligations of this Agreement is employed; coordinating any changes to this Agreement that might occur over the course of the Agreement; and, performing the closeout process when both Parties have met their obligations.

Authentication - the process by which an individual's identity is determined by verifying presented credentials. The authentication of a BCSC involves verifying the chip in the presented card, and generally includes a passcode or a photo validation.

Authoritative Party - an organization or individual that is trusted to be an authority on the identity related attributes or roles associated with users and subjects of services. Authoritative Parties may issue credentials. The IDIM program is the Authoritative Party of BC residents that are issued BC Services Cards.

Authorization - the process for determining and recording the permissions an individual has to access Protected Resources.

BC Services Card (BCSC) - a government ID and credential issued by the Province to individuals for identification and access to services. The card contains a security chip that can be used to electronically authenticate the cardholder when accessing in-person and online services.

BCSC Authentication Service –a provincial service to authenticate BCSC Cardholders and provide trustworthy identity information about the Cardholder to BCSC Client systems and staff.

BCSC Client - a ministry program, public sector program, or private sector program that uses the BCSC Authentication Service to support its online services to be delivered to End Users.

BC Services Card Login Service Terms of Use Agreement – an agreement between the Province of British Columbia and a BCSC Cardholder describing the terms agreed to regarding use of the BC Services Card login service.

Card Reader – an electronic device that can read plastic cards embedded with a barcode, magnetic strip, computer chip or another storage medium, such as the security chip on a BCSC. It can be a standalone device that connects to a computer via USB or it may be integrated into a computer, printer, or multifunction device.

CPPM - *Core Policy and Procedures Manual* that contains Province-wide policies for managing information, communication, material, transportation, contracts and expenses.

Credential - a physical or electronic object (or identifier) that is issued to, or associated with, an individual and attests to the truth of certain stated facts and/or confers a qualification, competence, status, clearance or privilege on that individual. The BCSC is both a physical and electronic credential that is issued by the Province that proves an individual's identity information.

Employee - in relation to a public body, includes (a) a volunteer, and (b) a service provider.

End User - an individual who accesses BCSC Authentication Services as, or on behalf of, a BCSC cardholder.

FOIPPA - the *Freedom of Information and Protection of Privacy Act* (British Columbia).

Government - means Her Majesty the Queen in right of the Province of British Columbia.

Identity Information Management - a set of principles, practices, policies, processes and procedures that are used within an organization to manage identity information and realize desired outcomes concerning identity.

IDIM Program – a program established in July 2012 by the Office of the Chief Information Officer (OCIO). The program's mandate is to deliver secure and privacy-enhancing identity services for citizens and businesses to support access to government services and information.

Information - refers to Personal Information and/or Non-Personal Information.

Information Sharing Agreement (ISA) - an agreement that documents the terms and conditions of the exchange of Personal Information in compliance with the provisions of FOIPPA and any other applicable legislation.

Information Security Policy – operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of Province services, including those listed in Schedule B.
(See *http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf* for more information.)

Information Sharing Requirements – the requirements set out in Schedule A.

Intellectual Property - refers to intangible (non-physical) property, which includes copyright, moral rights related to copyrighted materials, trademarks, official marks, domain names, patents and industrial designs.

Non-Personal Information - recorded information that is not Personal Information

Online Service - a service delivered electronically to End Users.

Passcode - a secret numeric password that can be used with a BCSC to authenticate an individual, similar to a PIN with a bank or credit card.

Personal Information - means recorded information about an identifiable individual other than contact information (as defined in FOIPPA). (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.)

Privacy Impact Assessment (PIA) - a foundation tool/process designed to ensure compliance with government's privacy protection responsibilities and is a requirement under section 69(5) of FOIPPA.

Privacy Management Program (PMP) - - as set out in the Privacy Management and Accountability Policy issued by the OCIO.

Protected Resource – a resource that may only be accessed after successfully satisfying the terms of an access policy.

Province – means Her Majesty the Queen in right of the Province of British Columbia.

Security Threat and Risk Assessment (STRA) - a structured method for gathering threat profile information to determine the adequacy of current safeguards from the point of view of requirements, efficiency and cost. Assessments suggest where to avoid, reduce and accept risk, as well as diminish the impact of threatening events. The STRA aligns with the CPPM and ISP for policies relevant to protecting electronic information and associated technology.

Service Provider - a person retained under a contract to perform services for a public body.

SiteMinder - the BC government centralized web access management system that enables user authentication and single sign-on, and auditing of access to web applications.

Third party network gateway (3PNG) - a private, secured network connection between the internal BC government communications network (SPAN/BC) and the communications network of a third party operating an electronic service on behalf of the BC government.

3. Interpretation

3.1. References to IDIM in this Agreement include any person duly authorized to act on behalf of the Provincial IDIM Program.

3.2. References to the BCSC Client in this Agreement include any person duly authorized to act on behalf of the <<Ministry>> <<Program Area>>.

3.3. References in this Agreement to any enactment includes all subordinate legislation under it, as may be amended, extended, re-enacted or replaced and in force for the time being, whether before or after the date of this Agreement.

3.4. References in this Agreement to a policy of the Province refers to that policy, including all referenced policies in it, as may be amended, supplemented or replaced and in effect for the time being, whether before or after the date of this Agreement.

4. BCSC Authentication Service

This Agreement covers the following authentication and identity information management services as needed by the BCSC Client and provided by IDIM. Any other service that the BCSC Client wishes to deliver using IDIM's BCSC Authentication Service requires a separate Agreement.

(NOTE: During the development of each Service Agreement, this list will be populated with the authentication and identity information management services needed by the BCSC Client.)

1.
2.

5. General Terms and Conditions

5.1. The Parties will comply with all legislation, regulations, policies and standards applicable to the BCSC Authentication Service, including without limitation those listed in Schedule B - Relevant Legislation and Policies.

5.2. Access to, and use of, the BCSC Authentication Service and Information by the BCSC Client is subject to applicable laws (including FOIPPA), this Agreement and attached Information Sharing Requirements (Schedule A), and any directives or policies of the Province that apply to the BCSC Authentication Service.

6. Limitations of Responsibility

IDIM and its service delivery partners will exercise due diligence to minimize the issuance of cards to fraudulent identities and ensure that identity information is accurate. The BCSC Client acknowledges that IDIM cannot be held liable for any errors that may arise.

7. IDIM Roles and Responsibilities

7.1. IDIM will:

7.1.1. Provide 24 hours a day, seven days a week BCSC Authentication Service (excluding planned outages, unforeseen outages and change windows);

7.1.2. Manage and maintain all data stored within IDIM;

7.1.3. Identify, implement, monitor, maintain, and enhance, as required, reasonable controls to meet the security and privacy obligations of the Province's security and privacy policies and legislation;

7.1.4. Complete and maintain PIAs for the BCSC Authentication Service;

7.1.5. Complete and maintain STRAs for the BCSC Authentication Service;

7.1.6. Maintain a business continuity plan and disaster recovery plan;

7.1.7. Appoint an Agreement Administrator;

7.1.8. Maintain a list of IDIM representatives who will liaise with the BCSC Client for service planning and operations;

7.1.9. Provide a primary contact point for BC Services Card program-related enquiries from citizens during business hours;

7.1.10. Inform End Users of best practices for protecting their BCSC, personal information and passcode, as well as measures for reducing the potential for identity fraud;

7.1.11. Assist the BCSC Client to support audits of the <Service Name>> on a cost recoverable basis, as authorized by the Information Sharing Requirements (Schedule A);

7.1.12. Immediately deactivate a BCSC, where the BCSC is reported lost, stolen or damaged, or where the identity information on the BCSC has been confirmed to be fraudulent; and

7.1.13. Procure card readers on behalf of the BCSC Client.

7.2. The BCSC Client will:

7.2.1. Manage the systems and communication infrastructure required to access the BCSC Authentication Service (for example, third party network gateway, workstations, servers, and networks);

7.2.2. Manage End User authorization and access control with their systems;

7.2.3. Implement and maintain required authorization and access security measures (for example, transaction encryption) that are supplemental to those provided by the BCSC Authentication Service;

7.2.4. Assume responsibility for the actions and activities of all employees and contracted Service Providers to which it has granted access to the BCSC Authentication Service Information;

7.2.5. Appoint an Agreement Administrator;

7.2.6. Provide and maintain an up-to-date listing of their representatives who will liaise with IDIM for service planning and operations;

7.2.7. Comply with the Corporate Privacy Management Program (PMP) administered by the Province's OCIO, and develop and implement any additional policies and practices required by the PMP;

7.2.8. Complete a PIA regarding their service in accordance with FOIPPA;

7.2.9. Complete a STRA regarding their service in accordance with the CPPM and ISP;

7.2.10. Provide IDIM with descriptions of their service's application and network architecture;

7.2.11. Obtain approval on the invitation to the public to access their service using the BCSC, from IDIM, 60 days in advance of its release;

7.2.12. Provide support to their End Users who have questions about the service or how to access it;

7.2.13. Assign one or more representatives to participate in service management processes;

7.2.14. Manage relationships with their auditors and convey auditor requests for information to IDIM, as authorized by the Information Sharing Requirements (Schedule A);

7.2.15. Work with IDIM regarding card reader requirements (e.g., volume and timing) and, if necessary, arrange for sufficient financing to procure readers.

8. MANAGEMENT OF INFORMATION

8.1. The Parties agree to comply with the Information Sharing Requirements set out in Schedule A of this Agreement, which details the Information to be shared on a regular and systematic basis between the Parties for the purpose of delivering the BCSC Client's service using the BCSC Authentication Service.

8.2. The BCSC Client agrees to enter into an Information Sharing Agreement, or to set similar conditions and requirements in a separate contract, with any other party that receives any Information set out in Schedule A of this Agreement. Any such information sharing must be compliant with the provisions of FOIPPA.

8.3. The Parties will make every reasonable effort to ensure the Information in their custody or control is accurate, complete and up-to-date.

8.4. The Agreement Administrators will designate contacts to assist the End Users with their right to request access or correction or annotation of, Personal Information about themselves or someone they act on behalf of (as defined in FOIPPA).

8.5. The Parties' employees will have a level of access to Information based on the requirements of their positions. When an employee changes position with IDIM or the BCSC Client, that employee's access to Information shall be immediately altered to reflect his/her new requirements or, immediately terminated if access is no longer required.

8.6. The Parties' will take all reasonable steps to ensure that employees who cease employment with their employer will maintain the confidentiality of the Information to which they have been privy.

8.7. The Parties will establish monitoring and reporting procedures regarding information management.

8.8. The Parties acknowledge that they will comply with Office of the CIO's (OCIO's) information incident management process in the event of any breach of privacy. (Go to *http://www.cio.gov.bc.ca/cio/information_incident/index.page?* for further information.)

8.9. The Parties will immediately report an actual or suspected privacy or security breach to the OCIO and follow all policies and processes set out in the OCIO's *Information Incident Management Process* and *Process for Responding to Privacy Breaches* (dated September 2011 and available at www.cio.gov.bc.ca/cio/information_incident/index.page), related to:

(a) The privacy of individuals; and/or,
(b) The security of any system in their respective custody or control that is used to access or store the Information covered by this Agreement.

(As set out in Section 69.2(3) of FOIPPA)

8.10. The Parties agree that for the purposes of auditing access, they will retain audit logs of electronic access to Information covered by this Agreement:

(a) According to the approved records retention schedule for the system or information asset; and,
(b) Indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

(Source: *http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf*)

9. Ownership, Intellectual Property and Retention

9.1. All intangible (non-physical) property, which includes copyright, moral rights, related to copyrighted materials, trademarks, official marks, domain names, patents and industrial designs provided to the BCSC Client in respect of the BCSC Authentication Service will constitute Intellectual Property. Parties agree to protect the Province's Intellectual Property.

9.2. The BCSC Client acknowledges that Information it receives from IDIM may be of a secure or sensitive nature and agrees not to distribute such Information to any third party without the prior written approval of IDIM. Any disclosure without IDIM approval will constitute a breach (see section 8.9).

9.3. The Parties will ensure that information collected by them will be managed and retained according to government records management standards.

10. Annual Review

The Parties will review this Agreement and the Information Sharing Requirements that are attached to, and form part of, this Agreement, one year after signing, and annually thereafter.

11. Other Reviews and Revisions

11.1. This Agreement may not be amended except by written agreement of the Parties.

11.2. Either Party may request a review of this Agreement, at any time.

11.3. The Party requesting the review will provide written notification and description of the requested revision to the other Party.

11.4. The Parties will meet promptly to discuss and negotiate required revisions to the Agreement.

11.5. Failure to reach an agreement after a 30-day negotiation period will require the Parties to agree to an extension, or the initiation of the dispute resolution process described in section 12.

11.6. The terms of the original Agreement will remain in force until the dispute is resolved, or the Agreement is terminated under section15.

12. Dispute Resolution

The Parties agree to undertake their best efforts to resolve any dispute arising out of, or in connection with, this Agreement in an amicable and expeditious manner through the following steps, in sequence:

12.1. Discussion between the Agreement Administrators;

12.2. Referral to their executives;

12.3. Referral to their assistant deputy ministers; and

12.4. Referral to their deputy ministers.

13. Suspension of <<BCSC Client's>> use of BCSC Authentication Service

13.1. IDIM may suspend BCSC Authentication Service to the BCSC Client, without notice, if the BCSC Client:

13.1.1. Contravenes the terms and conditions of this Agreement;

13.1.2. Otherwise jeopardizes the operation or security of the BCSC Authentication Service; or,

13.1.3. For administrative reasons.

13.2. IDIM may in its sole discretion resume providing BCSC Authentication Service to the BCSC Client upon confirmation that the BCSC Client has remedied the reason(s) for the suspension of service.

14. Suspension or Termination of an End User's Access to BCSC authentication service

IDIM may at any time at its sole discretion suspend or terminate an End User's access to the BCSC Authentication Service, if:

(a) The End User does not follow the BC Services Card Login Service Terms of Use Agreement;
(b) As a security measure; or,
(c) For administrative purposes.

15. Term and Termination of Agreement

15.1. Unless terminated earlier or extended under another section, the term of this Agreement will commence on the date of signing of this Agreement by both Parties, and will continue in effect until such time as either Party terminates this Agreement or both Parties mutually agree to terminate this Agreement.

15.2. The BCSC Client may terminate this Agreement immediately if IDIM fails to meet its obligations under this Agreement, provided the BCSC Client ceases to use the BCSC Authentication Service following termination.

15.3. Upon termination of the Agreement, the BCSC Client will return to IDIM, or securely destroy and provide evidence of such destruction to IDIM, any of the Information referred to section 9.2.

16. Survival of Obligations Upon Termination of Agreement

Upon termination of this Agreement, the protection, privacy, confidentiality and security provisions set out in this Agreement will continue to apply to the Information disclosed under this Agreement.

17. Cost Recovery

Cost recovery obligations related to the use of the BCSC Authentication Service are not addressed in this Agreement. Cost recovery for the use of the BCSC Authentication Service shall be determined by the governing bodies of IDIM, as approved by Treasury Board.

18. APPROVALS

Signed on behalf of the Minister of <<Ministry Name>>

Agreement Administrator:	<<Name>> <<Title>> {BUSINESS - Director/Manager} <<Program Area>>	Date

Signed on behalf of the Minister of Technology, Innovation and Citizens' Services

Agreement Administrator:	Lynda Hoel Director, Service Operations Provincial IDIM Program Ph: 250 356-9101 Lynda.hoel@gov.bc.ca	Date

SCHEDULE A - INFORMATION SHARING REQUIREMENTS

PURPOSE

1. The purpose of this Schedule is to establish the terms and conditions of the exchange of Information between the Parties that is necessary to collaboratively deliver the BCSC Client's service using the BCSC Authentication Service.
2. To support the Parties' commitment to privacy protection and compliance with FOIPPA, this Schedule sets out the Information that will be exchanged, the purpose of the exchange and, if applicable, the section of FOIPPA that authorizes the exchange.
3. This Schedule also sets requirements for protecting the security of the Information that is exchanged between the Parties including requirements relating to compliance monitoring and investigations.

SCOPE

4. This Schedule sets out the terms and conditions of the regular and systematic exchange of Information between the Parties that is necessary for the Parties to discharge their respective and collective roles and responsibilities related to the BCSC Authentication Service.
5. The Information covered by this Schedule, and the purposes for which the Parties agree to exchange it, are set out in sections 9 to 12 of this Schedule.
6. In addition to the regular and systematic exchange of Personal Information between the Parties, as described in this Schedule, it may be necessary on a case-by-case basis to collect, use and disclose additional Personal Information necessary to deliver the services. The Parties will ensure that these additional collections, uses or disclosures are authorized by section 26, 32, or 33 of FOIPPA.
7. If the collection, use or disclosure of Information not set out in this Schedule becomes regular and systematic, the Parties agree that this Schedule will be amended to include the regular and systematic new collection, use or disclosure.

GENERAL REQUIREMENTS

8. With respect to Personal Information exchanged under this Schedule, the Parties acknowledge their responsibility to meet the protection of privacy requirements set out in Part 3 of FOIPPA. While additional requirements may be established by this Schedule, they may not diminish the requirements set out in Part 3 of FOIPPA or in any way limit the ability of the Parties to meet the requirements set out in Part 3 of FOIPPA.

INFORMATION SHARED BY IDIM WITH THE BCSC CLIENT

9. IDIM agrees to disclose, under section 33.1 (5) of FOIPPA, the following elements of Personal Information as required by the BCSC Client in the delivery of <<Service Name>> for the specific use identified below.

(NOTE: During development of each Service Agreement, this list will be customized to the elements required by the BCSC Client to provide<<Service Name>>.)

	Elements of Personal Information	*Purpose of Use in the delivery of <<Service Name>>*
1.	**Primary Documented Surname -** The individual's documented surname recorded from valid identification.	
2.	**Primary Documented Given Name -** The individual's documented given names recorded from valid identification.	
3.	**User Display Name -** The individual's name which is their preferred name if available or composed of their documented name.	
4.	**Birth Date -** The individual's documented birth date recorded from valid identification.	
5.	**Age -** The individual's age in years based on the documented birth date recorded from valid identification.	
6.	**Age 19 or Over -** An indicator of whether the individual's age is 19 years or greater based on the documented birth date recorded from valid identification.	
7.	**Sex -** The individual's documented sex or gender recorded from valid identification.	
8.	**Street Address -** The street address lines of an individual's provided residential address.	
9.	**Locality -** The city, municipality or district of an individual's provided residential address.	
10.	**Province -** The two-letter province code of an individual's provided residential address.	
11.	**Postal Code –** The postal code of the individual's provided residential address.	
12.	**Country –** The two-letter country code of an individual's provided residential address.	
13.	**Address Block –** All address lines of the individual's provided residential address.	
14.	**Verified Email –** The email address provided by an individual that has been verified with email delivery once.	

10. With respect to the Personal Information set out in section 9 of this Schedule, the BCSC Client agrees to collect it from IDIM under section 26(h)(ii) of FOIPPA and to only use it for the purpose specified to provide <<Service Name>> .

11. IDIM agrees to disclose to the BCSC Client the following elements of Non-Personal Information as required by the BCSC Client in the delivery of <<Service Name>> for the specific use identified below.

(NOTE: During development of each Service Agreement, this list will be customized to the elements required by the BCSC Client to provide<<Service Name>>.)

	Elements of Non-Personal Information	*Purpose of Use in the delivery of <<Service Name>>*
1.	**User Type** - The type of user that was authenticated. For BC Services Card, this will have the following value: "**Verified Individual**".	
2.	**User Identifier** - An identifier issued by one party for the sole use of another party. It must be unique within the issuing party. It must be opaque so it cannot infer any information about the individual except its existence and uniqueness.	
3.	**Transaction Identifier –** A unique identifier of the transaction that was used to authenticate the individual.	
4.	**Identity Assurance Level –** The level of confidence in the certainty of the identity claims of the individual according to the OCIO Identity Assurance Standard.	
5.	**Identity Assurance Level 1 –** An indicator, true or false, that there is a level 1 confidence in the identity claims of the individual according to the OCIO Identity Assurance Standard.	
6.	**Identity Assurance Level 2 –** An indicator, true or false, that there is a level 2 confidence in the identity claims of the individual according to the OCIO Identity Assurance Standard.	
7.	**Identity Assurance Level 3 –** An indicator, true or false, that there is a level 3 confidence in the identity claims of the individual according to the OCIO Identity Assurance Standard.	

12. With respect to the Non-Personal Information set out in section 11 of this Schedule, the BCSC Client agrees to collect it from IDIM and to only use it for the purpose specified to provide <<Service Name>>.

SECURITY

13. The Parties agree to make reasonable arrangements to protect the security of the Information disclosed to it or its Service Providers, or contracted Service Providers, under this Schedule against such risks as unauthorized access, collection, use, disclosure or disposal.

14. In addition to the provisions of sections 8.8 and 8.9, the Parties agree to immediately notify each other of any circumstances, incidents or events which to their knowledge have jeopardized or may jeopardize:

    (a) The privacy of individuals; and/or,
    (b) The security of any system in their respective custody or control that is used to access or store the Information covered by this Schedule.

15. The Parties agree to protect the security of Information during electronic transmissions by meeting or exceeding the requirements contained in the OCIO Cryptographic Standards for Information Protection at *http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf*

16. The Parties agree :

    (a) That access to Information covered by this Schedule is only authorized where the access is necessary to deliver the services described in Section 1 of this Agreement, and,
    (b) To ensure that individuals who are authorized to access Information covered by this Schedule are:
        1. Aware of their responsibilities and legal requirements and/or obligations under FOIPPA to protect that Information from unauthorized access, collection, use, disclosure or disposal; and,
        2. Provided adequate training on protecting Personal Information.

SCHEDULE B - RELEVANT LEGISLATION AND POLICIES

The Parties will, without limiting their obligation to comply with other relevant legislation and policies, comply with the following Provincial legislation, regulations, policies and standards as they apply to the BCSC Authentication Service and participating services, and as amended from time to time.

This list is not exhaustive and additional applicable legislation and policies may be added as required.

Chief Information Officer's Directives

Core Policy and Procedures Manual

Document Disposal Act

Electronic Transactions Act

Financial Administration Act

Freedom of Information and Protection of Privacy Act

Minister's Directions to the Provincial Identity Information Services Provider

Information Security Policy

IM/IT Standards Manual, which includes the Cryptographic Standards for Information Protection and the Identity Information Management Standards

BC Public Service Standards of Conduct

Public Service Act