IDENTITY AND AUTHENTICATION SERVICES
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>>
(CLIENT)

Each referred to as a "Party" and collectively as the "Parties"

TABLE OF CONTENTS

1. PURPOSE

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

This Service Agreement (the Agreement) sets out the details concerning the Client's access and use of IDIM's Identity and Authentication Services 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 IDIM's Identity Authentication Services.

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

2. IDIM'S IDENTITY AND AUTHENTICATION SERVICES

This Agreement covers the following IDIM's Identity and Authentication Services as needed by the Client to provide the services identified in the Schedules of this 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 Client.)

1.
2.
3.

3. GENERAL TERMS AND CONDITIONS

3.1. The Parties will comply with all legislation, regulations, policies and standards applicable to IDIM's Identity and Authentication Services, including those listed in Schedule - Relevant Legislation and Policies.

3.2. Access to, and use of, the information provided by IDIM's Identity and Authentication Services by the Client is subject to applicable laws (including where applicable FOIPPA), this Agreement (including schedules) and any government directives or policies that apply to IDIM's Identity and Authentication Services.

4. 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 Client acknowledges that IDIM is not responsible for any errors that may arise.

5. ROLES AND RESPONSIBILITIES

5.1. IDIM will:

a) Provide 24 hours a day, seven days a week, IDIM's Identity and Authentication Services (excluding outages and change windows);

b) Manage and maintain all data stored within IDIM;

c) Identify, implement, monitor, maintain, and enhance, as required, reasonable controls to meet the Province's security and privacy obligations;

d) Complete and maintain PIAs for IDIM's Identity and Authentication Services;

e) Complete and maintain STRAs for IDIM's Identity and Authentication Services;

f) Maintain a business continuity plan and disaster recovery plan;

g) Appoint an Agreement Administrator;

h) Maintain a list of IDIM representatives who will liaise with the Client for service planning and operations;

i) Provide a primary contact point for IDIM Program-related enquiries from citizens during business hours;

j) Inform End Users of best practices for protecting their credential, personal information and password/passcode, as well as measures for reducing the potential for identity fraud;

k) Assist the Client to support audits of the <Service Name>> on a cost recoverable basis, as authorized by the Information Sharing Requirements Schedule attached;

l) Immediately deactivate a credential, where the identity information of the credential has been confirmed to be fraudulent; or

(1) where the BCSC is reported lost, stolen or damaged

(2) where the BCeID password has been compromised; and

m) Procure card readers on behalf of the Client if applicable.

5.2. The Client will:

a) Manage the systems and communication infrastructure required to access IDIM's Identity and Authentication Services (for example, third party network gateway, workstations, servers, and networks);

b) Manage End User authorization and access control with their systems;

c) Implement and maintain required authorization and access security measures (for example, transaction encryption) that are supplemental to those provided by IDIM's Identity and Authentication Services;

d) Assume responsibility for the actions and activities of all Employees and contracted Service Providers to which it has granted access to the information provided by IDIM 's Identity and Authentication Services;

e) Appoint an Agreement Administrator;

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

g) Comply with the Privacy Management and Accountability Policy ("PMAP") administered by the Ministry of Finance, and develop and implement any additional policies and practices required by the PMAP;

h) Complete a PIA regarding their service in accordance with FOIPPA;

i) Consult with the Office of the Privacy, Compliance and Training Branch as required under FOIPPA or as directed by the OCIO;

j) Complete a STRA regarding their service in accordance with the CPPM and ISP;

k) Provide IDIM with descriptions of their service's application and network architecture;

l) Obtain approval from IDIM on any invitation to the public to access the Client's service using IDIM credentials, at least 60 days in advance of any such public access;

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

n) Assign one or more representatives to participate in service management processes;

o) Manage relationships with their auditors and convey auditor requests for information to IDIM, as authorized by the Information Sharing Requirements schedule attached;

p) Work with IDIM regarding BCSC card reader requirements (e.g., volume and timing) and, if requested, agree with IDIM to take part in financing the procurement of readers for citizens.

q) Register any online service using BCeID in the BCeID online service directories;

r) Inform IDIM at least 90 days prior to implementing any changes that will result in a significant increase in End Users;

6. MANAGEMENT OF INFORMATION

6.1. The Parties agree to comply with the Information Sharing Requirements set out in this Agreement, which detail the Information to be shared on a regular and systematic basis between the Parties for the purpose of delivering the Client's service using IDIM's Identity and Authentication Services.

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

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

6.4. 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 Client, that Employee's access to Information shall be altered to reflect his/her new requirements or, terminated if access is no longer required as soon as practicable.

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

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

6.7. The 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 Management of Information).

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

6.9. 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.

7. PRIVACY

7.1. With respect to Personal Information exchanged under this Agreement, 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 in the

Schedules, these additional requirements may not diminish the requirements set out in Part 3 of FOIPPA or in any way limit the ability for the Parties to meet the requirements set out in Part 3 of FOIPPA.

7.2. The Parties will immediately report an actual or suspected privacy or security breach and will follow all policies and processes set out in the Information Incident Management Process and Process for Responding to Privacy Breaches ("Incident Management Process"), 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.

7.3. The Parties acknowledge that they will comply with the Incident Management Process in the event of any breach of privacy

8. SECURITY

8.1. The Parties agree to make reasonable arrangements to protect the security of the Information disclosed to them or their service providers against such risks as unauthorized access, collection, use, disclosure or disposal.

8.2. 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.

(See: http://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/office-of-the-chief-information-officer)

8.3. The Parties agree:

(a) That access to Information covered by this Agreement is only authorized where the access is necessary to deliver the services described in the Schedules of this Agreement; and;

(b) To ensure that individuals who are authorized to access Information covered by this Agreement 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.

9. ANNUAL REVIEW

The Parties will review this Agreement (including Schedules) annually.

10. Other Reviews and Revisions

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

10.2. Either Party may request in writing a review of or a revision to this Agreement, at any time, and provide a description of any requested revision to the other Party.

10.3. The Parties will meet promptly to discuss any requested revisions to the Agreement.

10.4. If the parties cannot agree to any requested revisions within 30 days following the receipt of the request for revision, either Party may initiate the dispute resolution process described below.

11. Dispute Resolution

The Parties agree to undertake their best efforts to resolve any dispute under this Agreement in an amicable and expeditious manner through the following steps, in sequence:

11.1. Discussion between the Agreement Administrators;

11.2. Referral to their Executives;

11.3. Referral to their Assistant Deputy Ministers; and

11.4. Referral to their Deputy Ministers.

12. Suspension or termination of services

12.1. IDIM may suspend IDIM's Identity and Authentication Services to the Client, immediately without notice:

a) If the Client contravenes the terms and conditions of this Agreement; or

b) If IDIM believes, in its sole discretion, the operation or security of IDIM's Identity and Authentication Services are jeopardized.

12.2. IDIM may suspend its Identity and Authentication Services to the Client, with 120 days written notice, for any other reason.

12.3. IDIM may in its sole discretion resume providing its Identity and Authentication Services to the Client upon confirmation that the Client has remedied the reason(s) for the suspension of service.

12.4. IDIM may at any time at its sole discretion suspend or terminate an End User's access to IDIM's Identity and Authentication Services, if:

(a) The End User does not follow the applicable terms of use agreements. E.g. BC Services Card Login Service Terms of Use Agreement, BCeID Terms of Use Agreement;
(b) As a security measure, or;
(c) For any other reason.

13. Term and Termination of Agreement

13.1. 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.

13.2. The Client may terminate this Agreement immediately if IDIM fails to meet its obligations under this Agreement, provided the Client ceases to use IDIM's Identity and Authentication Services following termination.

13.3. Upon termination of the Agreement, the Client will securely destroy, and provide evidence of such destruction to IDIM, all of the Information accessed under this agreement

14. Cost Recovery

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

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

Agreement Administrator:	Sophia Howse Executive Director OCIO – Technology Solutions Ministry of Technology, Innovation and Citizens' Services Phone: 250-213-7855 Email: Sophia.Howse@gov.bc.ca	Date

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

Agreement Administrator:	<<Name>> <<Title>> {BUSINESS - Director/Manager} <<Program Area>>	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 Client's service using IDIM's Identity and Authentication Services.
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 IDIM's Identity and Authentication Services.
5. 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 appropriate sections of FOIPPA.
6. 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.

INFORMATION SHARED BY IDIM WITH THE CLIENT FOR USE OF BC SERVICES CARD AUTHENTICATION SERVICE

1. IDIM agrees to disclose, under section 33.1 (5) of FOIPPA, the following elements of Personal Information as required by the Client in the delivery of <<Service Name>> for the specific use identified below.
2. With respect to the Personal Information set out in section 1 of this Schedule, the Client agrees to collect it from IDIM under section 26(h) (ii) of FOIPPA and to use it only for the purpose of providing access to the <<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 name recorded from valid identification. (note: first name only)	
3.	**Primary Documented Given Names -** The individual's documented given names recorded from valid identification (note: first and middle names)	
4.	**User Display Name -** The individual's name which is their preferred name if available or composed of their documented name.	
5.	**Birth Date -** The individual's documented birth date recorded from valid identification.	
6.	**Age -** The individual's age in years based on the documented birth date recorded from valid identification.	
7.	**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.	
8.	**Sex -** The individual's documented gender recorded from valid identification.	
9.	**Street Address -** The street address lines of an individual's provided residential address.	
10.	**Locality -** The city, municipality or district of an individual's provided residential address.	
11.	**Province -** The two-letter province code of an individual's provided residential address.	
12.	**Postal Code –** The postal code of the individual's provided residential address.	
13.	**Country –** The two-letter country code of an individual's provided residential address.	
14.	**Address Block –** All address lines of the individual's provided residential address.	
15.	**Verified Email –** The email address provided by an individual that has been verified with email delivery once.	

3. IDIM agrees to disclose to the Client the following elements of Non-Personal Information as required by the Client in the delivery of <<Service Name>>.
4. With respect to the Non-Personal Information set out in this Schedule, the Client agrees to collect it from IDIM to provide its <<Service Name>>.

	Elements of Non-Personal Information (Provided by default to client)
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.	**User Identifier Type** – Describes the type of User Identifier that is being provided. Defaults to "DID" for Qualified/Directed Identifier.
4.	**Authentication Transaction Identifier –** A unique identifier of the transaction that was used to authenticate the individual.
5.	**Identity Assurance Level –** The level of confidence in the certainty of the identity claims of the individual according to the OCIO Identity Assurance Standard. Value returned will be either "**1, 2 or 3"**
6.	**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.
7.	**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.
8.	**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.
9.	**Authoritative Party Name** – The name of the authoritative party supplying the attributes. For BC Services Card it is "**IAS**" at this time.
10.	**Authoritative Party Identifier** – An identifier representing the authoritative party supplying the attributes. Typically provided in URN format.

INFORMATION SHARED BY IDIM WITH THE CLIENT FOR USE OF BCEID AUTHENTICATION SERVICE

This agreement applies to the data elements listed in the data sharing scenarios described for each BCeID account type below. Each scenario lists the only data elements that are to be shared under that scenario. There are no scenarios, other than those described below, under which personal information and non-personal information subject to this agreement will be shared.

Basic BCeID Account

Data Sharing Scenario #1.x – title

Participants

- xxxxx

Context

Enter context.

Use Case

Enter use case.

Access Constraints

Enter access constraints.

Data Elements Shared

Data Element	*Sharing Mechanism*	*Account Type of Requestor*	*Target Account*	*Target Query Type*

Personal BCeID Account

Data Sharing Scenario #2.x – title

Participants

- xxxxx

Context

Enter context.

Use Case

Enter use case.

Access Constraints

Enter access constraints.

Data Elements Shared

Data Element	*Sharing Mechanism*	*Account Type of Requestor*	*Target Account*	*Target Query Type*

Business BCeID Account

Data Sharing Scenario #3.x – title

Participants

- xxxxx

Context

Enter context.

Use Case

Enter use case.

Access Constraints

Enter access constraints.

Data Elements Shared

Data Element	*Sharing Mechanism*	*Account Type of Requestor*	*Target Account*	*Target Query Type*

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 legislation, regulations, policies and standards as they apply to IDIM's Identity and Authentication Services and participating services, all as may be amended or replaced from time to time.

BC Public Service Standards of Conduct

Chief Information Officer's Directives

Core Policy and Procedures Manual

Electronic Transactions Act

Financial Administration Act

Freedom of Information and Protection of Privacy Act

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

Information Incident Management Process

Information Management Act

Information Security Policy

Minister's Directions to the Provincial Identity Information Services Provider

Privacy Management and Accountability Policy

Public Service Act

SCHEDULE C - DEFINITIONS

In addition to terms defined throughout this Agreement, in this Agreement, the following terms have the following meanings:

Agreement Administrator – a senior representative authorized on behalf of each Party to sign this Agreement who is 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.

Basic BCeID Account– a BCeID account used to access online services that do not require verification of the individual's identity. Registration is completed entirely online.

BCeID Account– an identity record and credential (userID & password) issued by the Province to individuals for identification and access to online services. There are 3 account types: *Basic, Personal and Business.*

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.

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.

Business BCeID Account- a BCeID Account used to access online services, including services that require the organization's identity be corporately verified. End users act exclusively as authorized representatives of the organization and not in their personal capacity.

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.

Client - a ministry program, public sector program, Public Body program, or private sector program that uses IDIM's Identity and Authentication Services to support its online services to be delivered to End Users.

CPPM - the Province's *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 retained under contract to provide services to the Public Body.

End User - an individual who accesses online services.

FOIPPA - the *Freedom of Information and Protection of Privacy Act* (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 (ISP) – the Province's Information Security Policy available at: *http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy*

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

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 BCeID Account– a BCeID Account used to access online services where you are acting in an individual capacity. To obtain a Personal BCeID you will require in-person identity verification.

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

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

Public Body- means (a) a ministry of the government of British Columbia, (b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2 of FOIPPA, or (c) a local Public Body.

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.

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