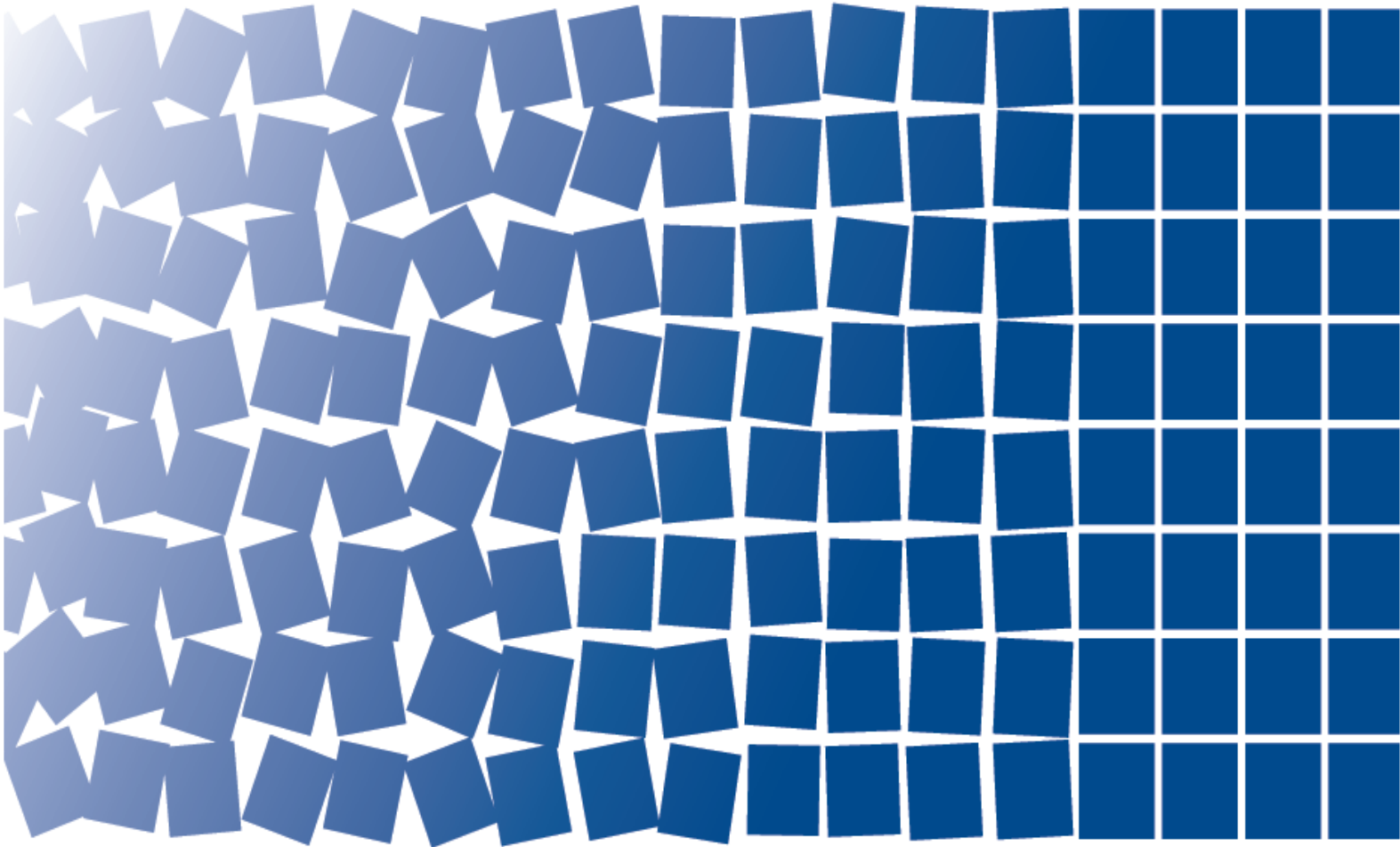


# BC SERVICES CARD PROGRAM OPERATIONAL RECORDS CLASSIFICATION SYSTEM



**GOVERNMENT RECORDS SERVICE**

# OPERATIONAL RECORDS CLASSIFICATION SYSTEM

---

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

## *BC SERVICES CARD PROGRAM*

### *OPERATIONAL RECORDS CLASSIFICATION SYSTEM*

#### TABLE OF CONTENTS

ORCS REGISTER OF AMENDMENTS

USEFUL INFORMATION

EXECUTIVE SUMMARY

SECTION 1      12000-12400

BC SERVICES CARD PROGRAM

SYSTEMS SECTION

## ORCS REGISTER OF AMENDMENTS

This register lists all approved changes made to the *BC Services Card Program ORCS*, in ascending order (i.e., the most recent changes appear first).

For more information about the changes listed here, see the relevant section, primary, and/or secondary; the *ORCS* may also have an appendix that provides a more detailed summary of changes.

**Original schedule approval date: 2018/11/08**

<b>Amendment Number</b>	<b>Amendment Type</b>	<b>Date Approved</b>	<b>Section/ Primary/ Secondary</b>	<b>Changes</b>
195736	Administrative	2023-10-23	Entire ORCS	Removed wording regarding previous service provider and chip technology.  ORCS formatted to align with ORCS 2020 standards.

## USEFUL INFORMATION

### Key to Information Schedule Codes and Acronyms:

Information Schedule titles:	<b>ARCS</b> = <i>Administrative Records Classification System</i> <b>ORCS</b> = <i>Operational Records Classification System</i>
Office information:	<b>OPR</b> = Office of Primary Responsibility
Records life cycle:	<b>A</b> = Active <b>SA</b> = Semi-active <b>FD</b> = Final Disposition
Active and semi-active period codes:	<b>CY</b> = Calendar Year <b>FY</b> = Fiscal Year <b>NA</b> = Not Applicable <b>SO</b> = Superseded or Obsolete <b>w</b> = week <b>m</b> = month <b>y</b> = year
Final disposition categories:	<b>DE</b> = Destruction <b>FR</b> = Full Retention <b>SR</b> = Selective Retention <b>OD</b> = Other Disposition <b>NA</b> = Not Applicable
Special flags:	<b>FOI</b> = Freedom of Information/Protection of Privacy <b>PIB</b> = Personal Information Bank <b>VR</b> = Vital Records

The following links provide additional resources for managing your information:

- [ARCS and ORCS User Guide.](#)
- [Special schedules for records that are not covered by ARCS and ORCS.](#)
- [Legislation, policies, and standards for managing records in the BC Government.](#)
- [Tips, guides, and FAQs on related topics.](#)
- [Government Records Officer contact information.](#)

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

---

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

### *BC Services Card Program*

### *Operational Records Classification System (ORCS)*

### Executive Summary For Amendment 1 - Administrative Amendment

#### **Creating Agency**

Ministry of Citizens' Services  
Office of the Chief Information Officer  
Provincial Identity Information Management (IDIM) Program

#### **Amendment Change Summary**

Amendment to remove references to "chips" and to the program's previous service provider.

#### **Scope**

The purpose of this amendment is to remove references to a previous technology and service provider, and to align formatting with ORCS 2020 standards.

#### **Endorsements**

Schedule Number: 144008                      Amendment Number: 195736

Schedule Developer: Elise Polkinghorne, Archivist, 2023-10-23

Approved by Director, Archives and Records Initiatives: Mario Miniaci, 2023-10-23

END OF EXECUTIVE SUMMARY



**INFORMATION SCHEDULE APPROVAL**

Title: *BC Services Card Program Operational Records Classification System (ORCS)*

Ministry of Citizens' Services

Technology Solutions/Provincial Identity Information Management (IDIM) Program

Scope of Schedule:

The *BC Services Card Program ORCS* establishes a classification system and retention and disposition schedule for the operational records created by the IDIM Program. The schedule covers records relating to developing and issuing a secure credential for BC residents to replace the Ministry of Health's CareCard. CITZ holds authority under the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165, s. 69.2) for issuing the BC Services Card, except for the combo card which is co-issued with the Insurance Corporation of BC under the authority of the *Motor Vehicle Act* (RSBC 1996, c. 318., s. 25). The *Medical and Health Care Services Regulation* (Reg. 53/2014) provides a complete description of the three types of BC Services Cards issued.

Records cover policy and program development files, identity management and authentication services data, and onboarding and business development files.

The retention periods specified in this schedule meet all operational, fiscal, legal, and audit requirements.

For more information, see the attached schedule.

Earliest date of records covered by this schedule: 2010

The government body endorses this schedule and its implementation.

See signed authorization authority

Assistant Deputy Minister, Office of the Chief Information Officer

Name: Ian Bailey

The Information Management Advisory Committee recommends this schedule for approval.

Susan Laidlaw, Chair

APPROVED BY THE CHIEF RECORDS OFFICER:

David Curtis

May 19, 2015

Date

Sep 19, 2018

Date

Nov 8, 2018

Date

*The attached schedule was developed in consultation with staff and managers who conduct the operational functions in the creating agency. It has also been reviewed by appropriate Government Records Service staff to ensure it meets scheduling and appraisal standards, and reflects sound recordkeeping practices.*

Schedule Developer: Sarah Jensen

Endorsed by Government Records Service.

Alexander Wright, Chief Archivist

Date

July 26, 2018

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

### SECTION 1

#### BC SERVICES CARD PROGRAM

#### PRIMARY NUMBERS

12000 – 12400

Section 1 covers records relating to developing and issuing a secure identification credential for BC residents to replace the Ministry of Health's CareCard used for provincial health insurance.

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

### SECTION 1 TABLE OF CONTENTS

#### BC SERVICES CARD PROGRAM

12000 - 12400

12000	BC SERVICES CARD PROGRAM - GENERAL
12200	BC SERVICES CARD PROGRAM - IDENTITY MANAGEMENT AND AUTHENTICATION SERVICES
12400	BC SERVICES CARD PROGRAM - ONBOARDING AND BUSINESS DEVELOPMENT



## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

### 12000 BC SERVICES CARD PROGRAM - GENERAL

Records that relate generally to the BC Services Card Program, which is an integrated program between the Ministry of Health (HLTH), the Insurance Corporation of BC (ICBC), and the Ministry of Citizens' Services (CITZ), not shown elsewhere in this schedule.

The program was launched on February 15th, 2013 through a multi-year project to develop and issue a secure identification credential for BC residents to replace the Ministry of Health's CareCard used for provincial health insurance.

Three types of credentials are issued: combination driver's license and BC Services Card ("combo"); BC Services Card with photo ("standalone"); and BC Services Card without a photo ("non-photo"). CITZ holds authority under the [Freedom of Information and Protection of Privacy Act \(RSBC 1996, c. 165, s. 69.2\)](#) for issuing the BC Services Card, except for the combo card which is co-issued by ICBC under the authority of the [Motor Vehicle Act \(RSBC 1996, c. 318, s. 25\)](#). The [Medical and Health Care Services Regulation \(Reg. 426/97\)](#) provides a complete description of the types of BC Services Cards issued and the agency responsible.

This primary covers policy and program development, customer support resource development, issues management, and reporting.

For BC Services Card web site, see [ARCS secondary 340-30](#).

For brochures and publications, see [ARCS primary 312](#).

For committee files, see [ARCS primary 200](#).

For final internal strategic and business plans, see [ARCS secondary 400-10](#).

For log files, see [ARCS secondary 6820-06](#).

For reference material/topical files, see [ARCS secondary 358-20](#).

For service agreements, see [ARCS secondary 146-45](#).

For surveys, see [ARCS primary 338](#).

For systems descriptions, see the System Overview

For system incidents, see [ARCS secondary 6820-25](#).

For training materials, see [ARCS primary 1735](#).

For User IDs and access authority files, see [ARCS secondary 470-40](#).

The ministry OPR is Provincial Identity Information Management (IDIM) unless otherwise noted below. See specific secondaries for OPR retention schedules.

12000	BC SERVICES CARD PROGRAM - GENERAL	A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
	<b>-00 Policy and procedures - final</b> (covers final/approved versions of policies, procedures, standards, and guidelines pertaining to the functions and activities documented in this Operational Records Classification Schedule (ORCS), developed for use by the program area and stakeholders)	SO	3y	FR
		(cont'd)		

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

12000	BC SERVICES CARD PROGRAM - GENERAL	A	SA	FD
	(includes terms of use documentation) (arrange by policy name or topic)			
	RETENTION STATEMENT Transfer to the government archives three years after the policy is replaced or becomes irrelevant.			
	SO: when the policy is replaced or becomes irrelevant			
	FR: The government archives will fully retain final versions of operational policy documentation because these provide significant evidence of the governance of the functions and activities covered by this ORCS.			
<b>-01</b>	<b>General</b>	CY+1y	nil	DE
	RETENTION STATEMENT Destroy at the end of the second calendar year.			
	NOTE: Throughout this section, this secondary covers miscellaneous records that relate to the primary but do not document decisions and actions, and do not relate to topics that warrant specific classifications.			
<b>-20</b>	<b>Customer support resources</b>	SO	nil	DE
	(covers resources including educational materials for the public, as well as job aids developed to support service delivery partners such as Service BC counter agents, contact centre staff, and Identity Analysts with their customer interactions) (includes quick reference guide, scripts, cardholder educational materials, and key messages) (arrange by topic)			
	RETENTION STATEMENT Destroy three years after the file is opened.			
	SO: three years after the file is opened			
	NOTE: Resources include suspected fraud management strategies for frontline staff.			

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

12000	BC SERVICES CARD PROGRAM - GENERAL	A	SA	FD
-30	<b>Issues management files</b> (covers counter agent or citizen reported incidents and general customer inquiries residing in a variety of tools such as SharePoint and Remedy, an incident tracking tool) (includes inquiries, correspondence, issues logs, and reports) (arrange by issue number or topic)  RETENTION STATEMENT Destroy six years after the issue is resolved or no longer topical and all fraud investigations are complete.  SO: when issue is resolved or no longer topical and all fraud investigations are complete  DE: These records have been appraised for destruction because issues of a significant nature are adequately documented under special schedule 102906 ( <a href="#">Executive Records</a> ).  NOTE: ICBC is the primary office of investigation for suspected fraud. ICBC notifies IDIM via a password protected email of card holders under investigation.  NOTE: The six-year semi-active retention period ensures the files are retained for the duration of the card lifecycle (five years) plus one additional year.  NOTE: System incidents will be classified under <a href="#">ARCS secondary 6820-25</a> .	SO	6y	DE
-35	<b>Policy development case files</b> (includes briefing notes, correspondence, process and procedural documents, terms of use drafts, and other working materials) (arrange by policy name or topic)  RETENTION STATEMENT Destroy two years after the policy is approved and distributed or abandoned.  SO: when the policy is approved and distributed or abandoned  DE: These records have been appraised for destruction because final policies are fully retained under secondary 12000-00.	SO	2y	DE

[Key to ARCS/ORCS Codes and Acronyms](#)

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

12000	BC SERVICES CARD PROGRAM - GENERAL	A	SA	FD
-40	<b>Program planning files</b> (covers BC Services Card Program foundational documents and other records documenting the development, monitoring, and evaluation of the program) (includes project files such as project charters, correspondence, meeting and communication materials, service descriptions/overviews, public consultation records, drafts, status reports, and other working documents) (arrange by topic)  RETENTION STATEMENT Transfer final BC Services Card and Identity Assurance Services (IAS) service descriptions/overviews to the government archives three years after the descriptions are no longer required for program planning, evaluation and review purposes or when the project is completed, abandoned or cancelled.  SO: when no longer required for program planning, evaluation and review purposes or when the project is completed, abandoned or cancelled  SR: The government archives will fully retain one copy of each final, completed version of BC Services Card and Identity Assurance Services (IAS) service descriptions/overviews in order to document the government's approach to providing citizens with secure access to a wide range of government services through one identity credential/card. Remaining program planning files will be destroyed  NOTE: Integrated project documentation is mainly housed on a SharePoint site managed by the Ministry of Health. Operational work is currently transitioning from Ministry of Health to IDIM.	SO	3y	SR

---

END OF PRIMARY

**OPERATIONAL RECORDS CLASSIFICATION SYSTEM**

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

**12200 BC SERVICES CARD PROGRAM - IDENTITY MANAGEMENT AND AUTHENTICATION SERVICES**

Records relating to the management and authentication of registered personal identity information and electronic credentials for citizens who are issued BC Services Cards stored in the Identity Assurance Services (IAS) system. The process of issuing a BC Services Card is a collaborative effort between the Insurance Corporation of BC (ICBC), the Ministry of Health/Health Insurance BC (HIBC), and the Identity Information Management (IDIM) program. ICBC is responsible for printing and registering BC Services Cards in the ICBC Drivers System and verifying client Medical Services Plan (MSP) eligibility with HIBC. HIBC is also responsible for determining whether citizens meet the exception or modified process criteria to receive a non-photo card. Once these steps are complete, ICBC sends encrypted identification and credential registration data to the IDIM program. The data is then reviewed for quality and registered in the IAS.

This primary covers IAS data management activities relating to personal identity and credential information, as well as credential usage and authentication profiles data.

For BC Services Card registration data, see special schedule 102901 ([Transitory Information](#))

For general system logging data, see [ARCS primary 6820](#).

For information system development and changes, see [ARCS secondary 6820-06](#)

For monthly card usage billing reports, see [ARCS secondary 1180-20](#).

For onboarding records, see primary 12400.

For operational policy, see secondary 12000-00

For privacy impact assessments, see [ARCS secondary 293-60](#).

For reference material/topical files, see [ARCS secondary 358-20](#).

For security, threat, and risk assessments, see [ARCS secondary 470-06](#)

For systems descriptions, see the System Overview

For system incidents, see [ARCS 6820-25](#).

For user access log data, see [ARCS secondary 470-40](#).

The ministry OPR is Provincial Identity Information Management (IDIM) unless otherwise noted below. See specific secondaries for OPR retention schedules.

<b>12200</b>	<b>BC SERVICES CARD PROGRAM - IDENTITY MANAGEMENT AND AUTHENTICATION SERVICES</b>	<b>A</b>	<b>SA</b>	<b>FD</b>
	All non-OPR offices will retain these records for:	SO	nil	DE
	<b>-01 General</b>	CY+1y	nil	DE

**RETENTION STATEMENT**

Destroy at the end of the second calendar year.

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

12200	BC SERVICES CARD PROGRAM - IDENTITY MANAGEMENT AND AUTHENTICATION SERVICES	A	SA	FD
-02	<b>Authentication profiles data</b> (covers authentication profiles stored in the IAS) (includes configuration profiles, service details, and identity attribute definitions specifying what can be provided from the IAS to the relying service)  RETENTION STATEMENT Destroy three years after termination of the service integration.  SO: upon termination of the service integration  NOTE: This configuration information is required to facilitate the login process to access online services.	SO	3y	DE
-03	<b>Credential management data</b> (covers information related to the card and electronic credential data) (includes lifecycle event records and credential binding metadata)  RETENTION STATEMENT Destroy seven and one-half years after the card or credential expires or is lost or stolen or has been replaced twice.  SO: when the card or credential expires or is lost or stolen or has been replaced twice  90m: The seven and half-year retention period is based on the Office of the Chief Information Officer (OCIO)'s <a href="#">Electronic Credential and Authentication Standard</a> .	SO+90m	nil	DE
-04	<b>Credential usage data</b> (covers card and electronic credential usage data logs, including every time IAS provides identity data to a relying service)  RETENTION STATEMENT Destroy upon expiration of data retention timelines as stipulated by ministerial direction for data recorded about which relying service was accessed, or for other credential usage data, three years after credential use.	SO	nil	DE

(cont'd)

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

<b>12200</b>	<b>BC SERVICES CARD PROGRAM - IDENTITY MANAGEMENT AND AUTHENTICATION SERVICES</b>	<b>A</b>	<b>SA</b>	<b>FD</b>
--------------	---	----------	-----------	-----------

---

- SO: final disposition triggers are as follows:
- for data recorded about which relying service was accessed, upon expiration of data retention timelines as stipulated by ministerial direction (see note)
  - for other credential usage data in this secondary, three years after credential use

NOTE: Current ministerial direction to the Provincial Identity Information Services Provider (Direction 1/12) states that the information recorded about which relying service was accessed is not retained for longer than 30 days unless the information is necessary for a privacy, security or fraud investigation.

---

<b>PIB</b>	<b>-05 Identity management data</b>	<b>SO+90M</b>	<b>nil</b>	<b>DE</b>
------------	-------------------------------------	---------------	------------	-----------

(covers the core identity data of a person issued a BC Services credential/card; unique identifiers representing each identity for use with partnering external systems and online services; activity alerts about technical incidents or suspected fraud logged in ID Check, a component of the IAS; and data mapping between identities and credentials/cards, and credentials/cards)

(includes personal identity information such as name, gender, date of birth, address, and card holder photograph; registration data such as identity proofing documentation; and identity registration date)

### RETENTION STATEMENT

Destroy seven and one-half years after the identity data is no longer required for identity management purposes or no longer needs to be accessed by authorized parties and all security and/or fraud investigations are complete.

SO: when identity data is no longer required for identity management purposes or no longer needs to be accessed by authorized parties and all security and/or fraud investigations are complete

90m: The seven and half-year retention period is based on the Office of the Chief Information Officer (OCIO)'s [Electronic Credential and Authentication Standard](#).

---

END OF PRIMARY

---

[Key to ARCS/ORCS Codes and Acronyms](#)



## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

### 12400 BC SERVICES CARD PROGRAM - ONBOARDING AND BUSINESS DEVELOPMENT

Records relating to establishing and managing relationships with BC Services Card clients through the process referred to as onboarding. Prospective clients such as government programs and services may access general information on how to use BC Services Card authentication services and the complete integration package, known as the onboarding kit, through the client authentication services web site. A client authentication solution, which may be integrated with existing online services, is developed by program area staff based on the differing business needs of clients. The purpose of the client authentication solution is to ensure organizations can verify the identity of their clients prior to providing access to their information or services.

These records document the program area's efforts to effectively communicate and market their services through the onboarding process, engage new and manage existing client relationships, and improve credential/card services through ongoing business development.

For business requirements documents, see [ARCS primary 6450](#).  
For client authentication services web site, known as the onboarding web site, see [ARCS secondary 340-30](#).

For identity management and authentication services, see primary 12200.  
For integrated program and service agreements, see [ARCS primary 146](#).  
For operational policy, see secondary 12000-00.  
For privacy impact assessments, see [ARCS 293-60](#).  
For reference material/topical files, see [ARCS secondary 358-20](#).  
For strategic planning documentation, see [ARCS primary 400](#).  
For systems descriptions, see the System Overview.

The ministry OPR is Provincial Identity Information Management (IDIM) unless otherwise noted below. See specific secondaries for OPR retention schedules.

12400	BC SERVICES CARD PROGRAM - ONBOARDING AND BUSINESS DEVELOPMENT	A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
	<b>-01 General</b>	CY+1y	nil	DE
	RETENTION STATEMENT Destroy at the end of the second calendar year.			
	<b>-05 Onboarding kit files</b> (covers informational and instructional onboarding kit materials such as templates and reports related to assisting clients with the onboarding process available on the BC Services Card client authentication services web site) (arrange by client integration stage)	SO	nil	DE
				(cont'd)

[Key to ARCS/ORCS Codes and Acronyms](#)



## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

12400	BC SERVICES CARD PROGRAM - ONBOARDING AND BUSINESS DEVELOPMENT	A	SA	FD
	<p>RETENTION STATEMENT</p> <p>Destroy when information is updated, no longer current, or the BC Services Card/credential ceases to exist.</p> <p>SO: when information is updated, no longer current, or the BC Services Card/credential ceases to exist</p> <p>NOTE: For records relating to the development of the onboarding/client authentication services, see business development files, secondary 12400-20.</p>			
-20	<p><b>Business development files</b></p> <p>(covers business development, planning, and evaluation records relating to such topics as client integration, engagement, and onboarding)</p> <p>(includes project charters, project plans, scope documents, correspondence, meeting and communication materials, drafts, and other working documents)</p> <p>(arrange by topic)</p> <p>RETENTION STATEMENT</p> <p>Destroy three years after implementation or abandonment of the project or program, or when the evaluation phase is complete, or when no longer required for onboarding planning or reference purposes.</p> <p>SO: upon implementation or abandonment of the project or program, or when the evaluation phase is complete, or when no longer required for onboarding planning or reference purposes</p>	SO	3y	DE
-25	<p><b>Client relationship management files</b></p> <p>(covers documentation relating to managing relationships with clients who onboard with the BC Services Card client authentication services)</p> <p>(includes contact information, completed onboarding templates such as letters of intent and integration checklists, correspondence, session planning notes, presentations, and related meeting materials)</p> <p>(arrange by client name and service)</p> <p>RETENTION STATEMENT</p> <p>Destroy three years after termination of service or when reference value has expired.</p>	SO	3y	DE

(cont'd)

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

**12400 BC SERVICES CARD PROGRAM - ONBOARDING AND BUSINESS DEVELOPMENT** **A SA FD**

---

SO: upon termination of service or when reference value has expired

NOTE: Completed service agreements will be classified under [ARCS secondary 146-45](#).

---

END OF PRIMARY

# OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

## BC SERVICES CARD PROGRAM

### OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

## SYSTEMS SECTION TABLE OF CONTENTS

<u>SECTION AND TITLE</u>	<u>PAGE NO.</u>
IDENTITY ASSURANCE SERVICES (IAS)	2

---

[Key to ARCS/ORCS Codes and Acronyms](#)

# OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

## IDENTITY ASSURANCE SERVICES (IAS)

### SYSTEM OVERVIEW

#### **Creating Agency**

Ministry of Citizens' Services  
Office of the Chief Information Officer  
Provincial Identity Information Management (IDIM) Program

#### **Date of System Description**

2023/10/23

#### **Purpose**

Identity Assurance Services (IAS) is IDIM's custom-built information system designed to support the BC Services Card (BCSC), a new type of government-issued identification, replacing the Ministry of Health's CareCard. The card is a physical credential that can be used to prove a set of facts about an individual, such as name and date of birth, and an electronic credential that can be authenticated for access to online services.

The purpose of the IAS is to securely manage registered personal identity information and electronic credentials of individuals who interact with government services. The IAS authenticates electronic credentials and provides identity information to relying government programs and services to help them deliver their services to their clients.

#### **Information Content**

The IAS contains the following data streams:

1. Identity data: personal identity information such as name, gender, date of birth, address, card holder photograph, registration data, and activity alerts relating to technical incidents or suspected fraud.
2. Credential data: identification information such as serial numbers; card and electronic credential lifecycle events such as activated, lost/stolen, or expired; and credential binding metadata linking cards and identities.
3. Credential usage data: records every time a credential is used or IAS provides identity data to a relying service.
4. Authentication profiles data: includes configuration profiles, service details, and identity attribute definitions specifying what can be provided from the IAS to the relying service.
5. User access log data: government workers accessing IAS applications such as ID Check.
6. General system logging data: normal system operations.

NOTE: Once the identity and credential data in the IAS is reviewed for quality, the source data from ICBC can be destroyed according to special schedule 102901 (Transitory Information).

#### **Inputs, Processes, and Outputs**

Inputs: IAS inputs consist of identity and credential registration data, account updates from partners, account updates directly from users, information entered by staff, configuration data for the system, and authentication profiles.

---

[Key to ARCS/ORCS Codes and Acronyms](#)

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

---

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

---

**Processes:** Identity and credential registration is the main form of data creation in the IAS. This includes issuance of the BC Services Card, and any of the other related credentials users may use with the identity and credential services of the IAS.

As the identity and associated credential move through their respective lifecycles, additional records are created to reflect the appropriate changes, including the source and reason for the change. Examples of this can include replacement/renewal/expiry of credentials and updates to identity information such as change of address.

As credentials are used, records are kept so that account activity can be displayed to the user, as well as to support subsequent reviews that they may request of suspicious activity. Identity records are also shared with client organizations at this time, so that they may record the user in their own systems based on the approved information sharing agreement and associated authentication profile within the IAS system.

**Outputs:** IAS outputs include identity data sent to the Ministry of Health's Client Registry during BC Services Card registration; monthly reports; identity information for client organizations; and system-generated correspondence sent to BC Services Card account holders based on user preferences (e.g., emails about account).

## OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2015, c. 27\)](#). For more information consult your [Government Records Officer](#).

### IDENTITY ASSURANCE SERVICES (IAS)

#### DATA RETENTION PLAN

Data Description	Data Retention Period
Authentication profiles data Classification 12200-02	Destroy three years after the termination of the service integration.
Credential management data Classification 12200-03	Destroy seven and one-half years after the card or credential expires or is lost or stolen or has been replaced twice.
Credential usage data Classification 12200-04	Destroy upon expiration of data retention timelines as stipulated by ministerial direction for data recorded about which relying service was accessed, or for other credential usage data, three years after credential use.
Identity management data Classification 12200-05	Destroy seven and one-half years after the identity data is no longer required for identity management purposes or no longer needs to be accessed by authorized parties and all security and/or fraud investigations are complete.

For additional classification details, including retention rationales, click on the links above.  
For descriptions of system related records (e.g. back-up data, log files, and transitory electronic data processing (EDP) records), see the [Systems Section FAQ](#).

END OF OVERVIEW

---

[Key to ARCS/ORCS Codes and Acronyms](#)