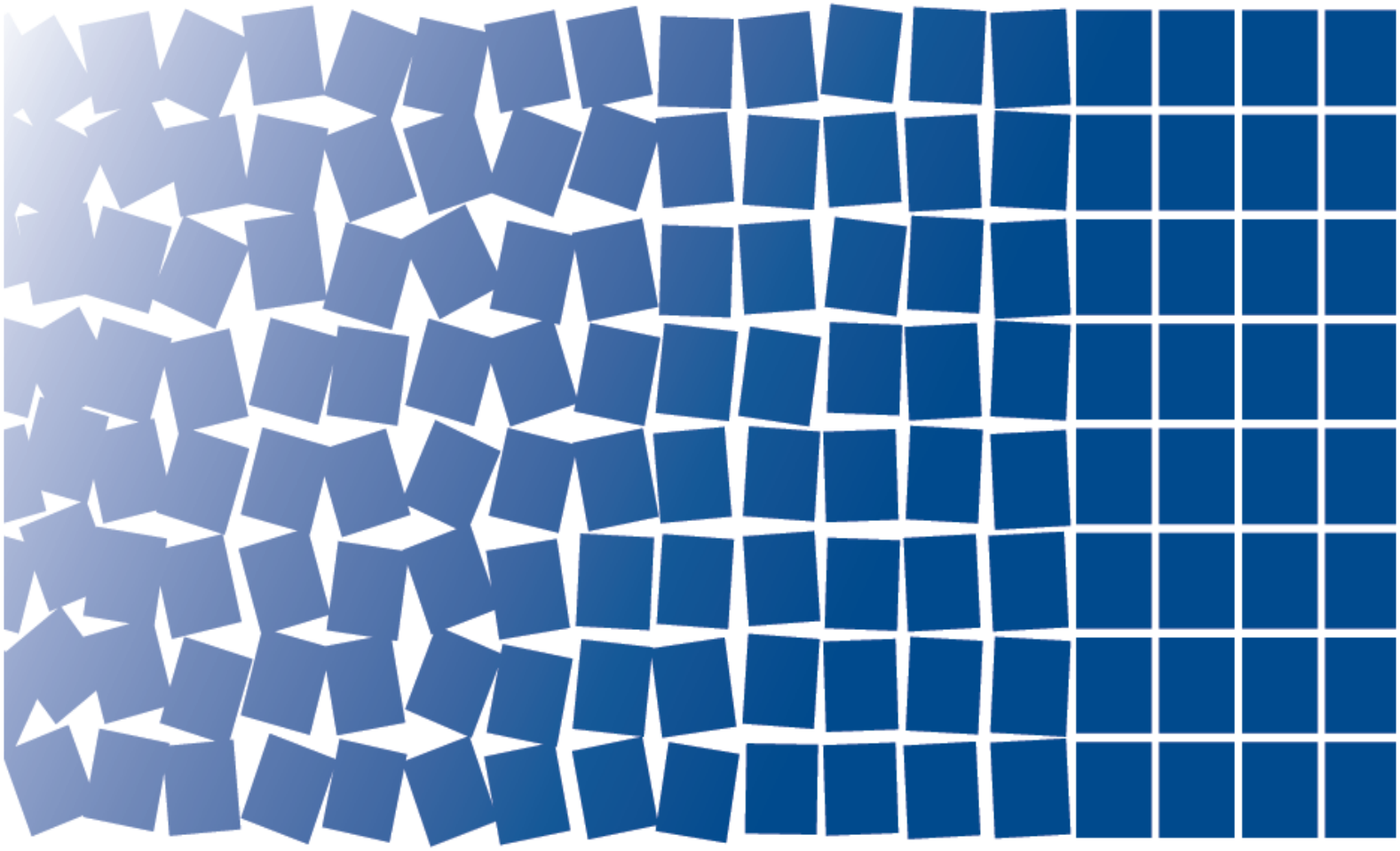
INFORMATION AND PRIVACY OPERATIONAL RECORDS CLASSIFICATION SYSTEM



BRITISH COLUMBIA

GOVERNMENT RECORDS SERVICE

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

INFORMATION AND PRIVACY

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

TABLE OF CONTENTS

INTRODUCTION

SECTION 1 30000-39999 INFORMATION AND PRIVACY

SYSTEMS SECTION

INDEX

ORCS REGISTER OF AMENDMENTS

This register lists all approved changes made to the *Information and Privacy ORCS*, in ascending order (i.e., the most recent changes appear first). Each amendment is uniquely identified as follows:

- **Formal amendments**: Schedule application number assigned to the amendment and used during the review and approval process; e.g., 123456.
- **Administrative amendments**: ADAM plus a registration number issued by Government Records Service (GRS); e.g., ADministrative AMendment number thirty-eight is ADAM 38.

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.

Unique identifier (ADAM # or Schedule #)	**Date Approved**	**Section/ Primary/ Secondary**	**Changes**
144018		Entire *ORCS*	Entire *ORCS* updated; See Appendix A for summary of changes.

BRITISH COLUMBIA Ministry of Citizens' Services

Schedule No: 194900
Amendment No: 144017

INFORMATION SCHEDULE APPROVAL

Title: *Information and Privacy Operational Records Classification System (ORCS) – Amendment 1*

Ministry of Citizens' Services
Privacy, Compliance and Training Branch (PCT)

Scope of Schedule:

This amendment to the *ORCS* reflects a variety of changes in Privacy, Compliance and Training's functional responsibility since the original *ORCS* was approved by the Legislature in 2008. Key changes include: introduction of investigative responsibility for information incidents, introduction of information management compliance assessments, and the transfer of responsibility for administration of the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) and the *Personal Information Protection Act* (SBC 2003, c. 63) to the Strategic Policy and Legislation Branch. Other amendments to primaries and secondaries have been made throughout the *ORCS* to include wording changes in scope notes, secondary titles, and secondary notes.

Classifications pertaining to functions which are now the responsibility of the Information Access Operations Branch have been removed and will be covered under a separate schedule.

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: 1987

The government body endorses this schedule and its implementation.

Authorizations on file — 08/29/2017
Acting Executive Directors– Privacy, Compliance and Training Branch — Date
Names: Matt Reed and Kenneth McLean

The Information Management Advisory Committee recommends this schedule for approval.

Susan Laidlaw — 06 Apr 2018
Susan Laidlaw, Chair — Date

APPROVED BY THE CHIEF RECORDS OFFICER:

[signature] — May 24/18
Name: David Curtis — 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: Chloe Powell

Endorsed by Government Records Service.

[signature]
Alexander Wright, Chief Archivist
Date 11/21/2017

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

A SA FD

INFORMATION AND PRIVACY

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

EXECUTIVE SUMMARY

This *Operational Records Classification System* (*ORCS*) amends the classification system and retention and disposition schedule for the operational records created by the Privacy, Compliance and Training Branch (PCT) in relation to the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) *(FOIPPA)*, the *Personal Information Protection Act* (SBC 2003, c. 63) *(PIPA)* and the *Information Management Act* (SBC 2015, c. 27).

PCT is the central office responsible for the delivery of information compliance and privacy services within the Government of British Columbia. This includes overseeing and facilitating privacy management activities across government; reviewing privacy impact assessments, information sharing agreements and privacy protection schedules; providing consultative support and liaison on government privacy initiatives and policy; informing and supporting the privacy legislation process; investigating information incidents, which include privacy breaches; and conducting information management compliance assessments.

This amendment to the *ORCS* reflects a variety of changes in PCT's functional responsibility since the original *ORCS* was approved by the Legislature in 2008. Key changes include: introduction of investigative responsibility for information incidents, introduction of information management compliance assessments, transfer of access functions to the Information Access Operations Branch, and the transfer of responsibility for administration of the *FOIPPA* and the *PIPA* to the Strategic Policy and Legislation Branch. Other amendments to primaries and secondaries have been made throughout the *ORCS* to include wording changes in scope notes, secondary titles, and secondary notes.

The active and semi-active retention periods specified in the schedule meet all operational, administrative, legal, fiscal, and audit requirements. The final dispositions have been reviewed to ensure that records having enduring evidential and historical values are preserved.

This *ORCS* amendment is retroactive and applies to all records (on-site and in off-site storage) which are in the custody and control of PCT.

The following summary describes new secondaries with a final disposition of selective retention or full retention and new secondaries with a retention period of seven years or greater. For a detailed description of all changes pertaining to this *ORCS* amendment, consult Appendix A: Summary of Changes to the *Information and Privacy ORCS*. In the following summary, records are linked to the *ORCS* by primary and secondary numbers.

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

	A	SA	FD
1) Central agency assessments - final products (secondary 30400-30)	SO	nil	SR

These records document a new function of government: information management compliance assessments. These assessments evaluate and monitor government's information management practices against relevant legislation and policy, and are completed by central agency auditors. Scheduled assessments include evaluations of each ministry, which are broad, high-level summaries of the level of compliance at the ministry level. Ad hoc assessments are completed by an auditor focused on specific areas of government in response to real and perceived incidents involving information management. The government archives will retain only scheduled assessments.

SO: when the following criteria are complete:

- for scheduled assessments, when assessment is complete, and three subsequent scheduled assessments have been completed
- for ad hoc assessments, when seven years has passed and no longer needed for research and reference purposes

SR: The government archives will fully retain scheduled assessments because they provide a concise, high-level summary of ministries' overall compliance with legislative requirements in the areas of privacy, access, records management, and information protection/security. Ad hoc assessments will be destroyed.

2) Research unit - reports and development files (secondary 30100-75)	SO	nil	SR

This secondary consists of cross-government research services provided by Research Decisions and Support Services (RDSS), a now defunct unit. RDSS's purpose was to increase informed decision-making across government. Ministries that did not have in-house policy or research teams hired RDSS to produce a final report to help inform policy, procedure or practice development activities. The branch no longer performs this function.

SO: when no longer required for research or reference purposes

SR: Reports and development files created by RDSS will be selectively retained. Prior to transfer to the government archives, branch staff will separate final reports from development files. Final reports will be fully retained; all other records will be destroyed. The government archives will fully retain the final reports because they consist of a unique collection of research reports used to inform policy and practice across government.

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

	A	SA	FD
3) Ministry self-assessments (secondary 30400-40)	SO+7y	nil	DE

These records document annual ministry-wide assessments in the areas of privacy, access, records management, and information protection/security, and are completed by all ministries of government.

SO: at the end of the calendar year in which the self-assessment is completed, plus an additional seven years

7y: The seven year semi-active retention period meets the operational and reference needs of the branch to have access to past assessments.

DE: Self-assessments have been appraised for destruction because the assessments are routine in nature, consisting simply of a maturity model filled out annually. In many cases, the information contained in a self-assessment is also duplicated in the scheduled assessments, which are fully retained (under secondary 30400-30).

4) Systems	SO	nil	DE

The Systems Section provides descriptions of electronic systems and classifications for the records residing on them. The data on the systems are described under the appropriate primary and secondary classifications.

Unless otherwise noted, each system will be destroyed when the records/data on it have been migrated to a new system performing the same function, or when the relevant retention schedules have elapsed, or the information has been preserved elsewhere.

END OF EXECUTIVE SUMMARY

USEFUL INFORMATION

Key to Information Schedule Codes and Acronyms:

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

SECTION 1

INFORMATION AND PRIVACY

PRIMARY NUMBERS

30000 – 39999

Section 1 covers records relating to the information and privacy management activities performed by the Privacy, Compliance and Training Branch (PCT) in relation to the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165), the *Personal Information Protection Act* (SBC 2003, c. 63), and the *Information Management Act* (SBC 2015, c. 27).

This section includes records relating to the following: overseeing and facilitating privacy management activities across government; reviewing privacy impact assessments, information sharing agreements, and privacy protection schedules; providing consultative support and liaison on government privacy initiatives and policy; informing and supporting the privacy legislation process; investigating information incidents, which include privacy breaches; and conducting information management compliance assessments.

SECTION 1 TABLE OF CONTENTS

INFORMATION AND PRIVACY

30000 - 39999

30000 INFORMATION AND PRIVACY - GENERAL

30100 INFORMATION AND PRIVACY ADVISORY SERVICES

30400 INVESTIGATIONS AND COMPLIANCE ASSESSMENTS

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

30000 INFORMATION AND PRIVACY - GENERAL

Records not shown elsewhere in the Information and Privacy Section that relate generally to the information and privacy activities perfomed by the branch under the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) and the *Personal Information Protection Act* (SBC 2003, c. 63).

This primary covers the development of internal policies and procedures, resources and operational tools, as well as the tools used to track the activities of the branch.

For annual reports, see *ARCS* secondary 400-02.
For briefing notes, see *ARCS* secondary 280-20.
For committee files, see *ARCS* secondary 200-20.
For final internal strategic and business plans, see *ARCS* secondary 400-10.
For ministerial orders, see *ARCS* secondary 140-50.
For orders in council, see *ARCS* secondary 140-60.
For program planning and performance files, see *ARCS* secondary 400-20.
For reference material/topical files, see *ARCS* secondary 358-20.
For websites and website management, see *ARCS* primary 340

The ministry OPR is the Privacy, Compliance and Training Branch unless otherwise noted below. See specific secondaries for OPR retention schedules.

30000	INFORMATION AND PRIVACY - GENERAL	A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-00	**Policies, procedures, and resources - final** (includes final internal policies and procedures, resources, and operational tools (e.g., guidelines, tip sheets, templates, forms, manuals, FAQs, directions, bulletins, and designations)) SO: when the policy is replaced or becomes irrelevant FR: The government archives will fully retain all final policies, procedures, and resources because they provide significant evidence of the government's privacy and compliance governance framework and the manner in which the branch informs the ministries of their rights and obligations under relevant legislation. NOTE: See secondary 30000-20 for the corresponding development files. NOTE: See secondary 30100-20 for privacy policies developed by clients and submitted to the branch for review.	SO	5y	FR
-01	**General**	CY+2y	nil	DE

Key to *ARCS/ORCS* Codes and Acronyms

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

30000	INFORMATION AND PRIVACY - GENERAL	A	SA	FD
-05	**Tracking spreadsheets and registers** (covers a variety of tools used to track the activities of the branch, including logs, indexes, spreadsheets, and registers (e.g. Privacy Helpline inquiry tracking sheet, PIA registers, conference attendees logs, and training tracking)) SO: when no longer required for tracking, reporting, or planning purposes NOTE: See secondary 30100-65for the Personal Information Directory.	SO	nil	DE
-20	**Policies, procedures, and resources - development files** (includes working materials, drafts, discussion papers, legal opinions, correspondence, copies of briefing notes, impact analysis of Privacy Commissioner's orders approval packages, and stakeholder feedback) (covers the development of records classified under secondary 30000-00 and secondary 30100-40) SO: when the policy, procedure, or resource is approved and distributed or abandoned DE: Policy, procedure, and resource development files may be destroyed because final versions are fully retained under secondary 30000-00 and secondary 30100-40.	SO	5y	DE

END OF PRIMARY

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

30100 INFORMATION AND PRIVACY ADVISORY SERVICES

Records relating to providing advice to clients (e.g., ministries; agencies, boards, and commissions; and the public) with respect to privacy issues such as: reviewing ministries' privacy impact assessments (PIAs); providing feedback and assistance with information sharing agreements (ISAs), research agreements, and privacy provisions in government contracts; receiving and notifying the appropriate bodies of foreign demands for personal information; and liaising with the Office of the Information and Privacy Commissioner (OIPC) on privacy issues.

The Privacy, Compliance and Training Branch (PCT) is responsible for the review of all PIAs conducted by government. The PIA process is used to evaluate and manage privacy impacts and to ensure compliance with privacy protection rules and responsibilities. It is a legislative requirement to complete a PIA in accordance with directions of the Minister responsible for FOIPPA when there is a development or change to an enactment, system, project, program or activity. The branch aids client ministries with the development of PIAs and assesses, issues recommendations, and reviews PIAs. A summary of completed PIAs are then listed on the Personal Information Directory (PID). The branch is also the central repository for all PIAs conducted by government.

The Freedom of Information and Protection of Privacy Act (FOIPPA) requires the Minister responsible for the *Act* to publish a directory that includes summaries of ISAs, PIAs, personal information banks (PIBs), health information banks (HIBs), and any other information the minister considers appropriate for each ministry. The PID documents the government's management of personal information holdings and assists the public in identifying the location of personal information about them held by government. The branch administers the PID, routinely updates it, and makes it available to the public.

FOIPPA also requires the head or an employee of a public body to immediately notify the Minister responsible for *FOIPPA* of a foreign demand or request for disclosure of personal information. This includes a subpoena, warrant, order, demand or request that is from a foreign court, foreign state or other foreign authority outside of Canada. Notifications of a foreign demand for disclosure are handled through the branch, which assesses the notification to determine whether further action is required from the Minister, develops a briefing note notifying the Minister of the request and any related responsibilities that the Minister may undertake, and then the branch issues acknowledgement of receipt to the notifying body.

Lastly, this primary also includes the records of the now defunct Research and Decision Support Services (RDSS) Unit, which was active from 2007 to 2012. RDSS operated as a corporate shared resource, providing research and decision support services for business planning, policy, and program development. Their deliverables included jurisdictional and organizational scans, literature reviews, and research on corporate-wide initiatives.

For briefing notes, see *ARCS* secondary 280-20.

For committees, see *ARCS* secondary 200-20.
For executive briefing notes, executive correspondence referral replies, and executive issues records, see *ARCS* primary 280.
For general inquiries, see *ARCS* primary 320.
For legal matters, including legal opinions, see *ARCS* primary 350.
For memoranda of understanding (MOUs), see *ARCS* primary 146.
For policies, procedures, and resources, see secondary 30000-00.
For procurement and contract management, see *ARCS* primary 1070.
For reviews and amendments of *FOIPPA* and *PIPA*, including amendments to schedules 2 and 3, see *ARCS* primary 140.

The ministry OPR is Privacy, Compliance and Training Branch unless otherwise noted below. See specific secondaries for OPR retention schedules.

30100	INFORMATION AND PRIVACY ADVISORY SERVICES	A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+2y	nil	DE
-04	**Foreign demands for disclosure** (includes reports, demands, responses, and briefing notes to the minister) (arrange by year, then by reporting public body) DE: These records have been appraised for destruction because records of significant findings and the resulting actions are adequately documented in executive records covered by special schedule 102906 (*Executive Records*), which are selectively retained. NOTE: Original branch briefing notes addressing foreign demands for disclosure may be classified under this secondary because they are routine in nature and do not warrant selective retention under *ARCS* secondary 280-20.	CY+2y	nil	DE
-20	**Client review and advice case files** (covers the following: review and advice activities provided by the branch in relation to client developed privacy policies, PIAs, common or integrated program agreements (IPAs) or activity agreements, research agreements, information sharing agreements (ISAs), contracts, and privacy protection schedules; provision of support to Ministry Privacy Officers; provision of support to ministries in their interactions with the OIPC; and lastly, liaison with the OIPC) (PIAs include initial reviews, substantive drafts, final signed assessments, and supporting documentation) SO: when the applicable following criteria have been met:	SO	5y	DE

30100	INFORMATION AND PRIVACY ADVISORY SERVICES	A	SA	FD

- For final signed PIAs, when the assessment is obsolete (e.g., when all the records described in the assessment are destroyed or when the PIA is replaced by a new version), and when no longer required for research and reference purposes; for cancelled files and unsigned drafts, when no longer required for research or reference purposes; for supporting documentation (e.g., IPAs, common activity agreements) and development files, when the associated PIA is signed off, and when no longer required for research and reference purposes
- For all other files, when no longer required for operational or reference purposes

5y: The five year semi-active retention period meets the operational and reference needs of the branch.

DE: These records have been appraised for destruction because records of significant findings, content, and the resulting actions are adequately documented in executive records classified under *ARCS* primary 280 and/or by special schedule 102906 (*Executive Records*).

NOTE: For final internal policies developed by PCT, see secondary 30000-00.

NOTE: See secondary 30000-05 for the Privacy Helpline inquiry tracking sheet.

-40	**Impact analysis of Commissioner's orders or investigations** (closed secondary - this function is no longer performed) (includes a copy of the Information and Privacy Commissioner's order or investigation) (arrange by calendar year) (covers the final analysis of the Information and Privacy Commissioner's orders or investigations)	CY+5y	nil	FR

FR: The government archives will fully retain the impact analysis of Commissioner's orders or investigations because they document the provincial government's interpretation of the order, and in combination with the final policies covered under secondary 30000-00, the analyses were used as a resource by ministries' staff when processing information access requests.

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

30100	**INFORMATION AND PRIVACY ADVISORY SERVICES**	**A**	**SA**	**FD**

NOTE: See secondary 30000-20 for the development records and approval packages pertaining to the final impact analysis.

NOTE: These records were created by the central agency to aid ministry staff in processing information access requests. The function is longer performed by government because similar information is now available online on the Privacy Commissioner's website.

-65	**Personal information directories and inventories** (includes the personal information directory (PID), directory of records (DOR), personal information inventories, development files, and correspondence)	SO	nil	DE

SO: when the applicable following criteria have been met:

- For the master PID, until the requirement to maintain the register is removed from *FOIPPA*; for previous/outdated versions of the PID, when replaced by three more recent versions (see note below)
- For the DOR, when no longer required to be maintained pursuant to *FOIPPA* (see note below)
- For inventories of government records, when no longer required to be maintained pursuant to policy
- For development files and correspondence, when no longer required to support the preparation of the directories and inventories

NOTE: Each month, the branch sends the updated PID register to DataBC for web publication. The branch retains the three most recent cycles of the register for data verification and correction purposes.

NOTE: When *FOIPPA* was initially passed in 1995, an annual index of records was required by the *Act*. In 2002, this requirement was removed. Therefore, the DOR is no longer produced.

NOTE: This secondary also covers data in the now defunct Personal Information Directory (PID) database.

-75	**Research unit - reports and development files** (closed secondary – this function is no longer performed)	SO	nil	SR

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

30100	INFORMATION AND PRIVACY ADVISORY SERVICES	A	SA	FD

(arranged by project)

(includes reports, tables, reviews, bibliographies, source material, drafts, and research notes)

(covers records produced by the now defunct Research and Decision Support Services unit and its predecessors ONLY)

SO: when no longer required for research or reference purposes

SR: Reports and development files created by the Research and Decision Support Services unit (RDSS) will be selectively retained. Prior to transfer to the government archives, branch staff will separate the final reports from the development files. The final reports will be fully retained; all other records will be destroyed. The government archives will fully retain the final reports because they consist of a unique collection of research reports used to inform policy and practice across government.

NOTE: RDSS, which operated from 2006 to 2012, offered cross-government research services. Their goal was to increase informed decision-making across government. Ministries that did not have in-house policy or research teams would hire RDSS to produce a final report to help inform policy, procedure or practice development activities.

END OF PRIMARY

30400 INVESTIGATIONS AND COMPLIANCE ASSESSMENTS

Records relating to the investigation of all actual and/or suspected information incidents (which includes breaches of privacy), as well as monitoring government bodies for compliance with established information management legislation and government policy.

An information incident is any event that threatens the privacy or security of government information. Information incidents include privacy breaches, which involve an access, collection, use, or disclosure of personal information that is contrary to *FOIPPA*. When an employee becomes aware of an actual or suspected government information incident, it must be reported to the Privacy, Compliance and Training Branch (PCT). Reports are received by the PCT's Investigations Unit through the Breach Reporting Line, the Privacy and Access Helpline, referrals from the Office of the Information and Privacy Commissioner, or through direct contact with the unit. The unit is responsible for the coordination, investigation and resolution of government information incidents.

Information management compliance assessments are undertaken to evaluate and monitor government's information management practices against relevant legislation and policy. Assessment types include: scheduled assessments (assessments at the Ministry level undertaken by auditors), self-assessments (annual assessments at the ministry level completed by all ministries), and ad hoc assessments (completed by an auditor focused on specific areas of government in response to real and perceived incidents involving information management).

For briefing notes, see *ARCS* secondary 280-20.
For client ministries' copies of assessments and compliance review records (e.g., scheduled assessments, self-assessments, and ad-hoc assessments) see *ARCS* secondary 975-40.
For client ministries' copies of investigations (e.g., privacy breach records), see *ARCS* secondary 293-50.
For committee files, see *ARCS* secondary 200-20.
For development of legislation and regulation, see *ARCS* primary 140.
For executive issues, including final issues reports, see *ARCS* secondary 280-40.
For final internal strategic and business plans, see *ARCS* secondary 400-10.
For policies, procedures, and resources, see secondary 30000-00.
For program planning and performance files, see *ARCS* secondary 400-20.
For reference material/topical files, see *ARCS* secondary 358-20.
For system description, see the systems section.
For systems operations, see *ARCS* primary 6820.

The ministry OPR is the Privacy, Compliance and Training Branch unless otherwise noted below. See specific secondaries for OPR retention schedules.

30400	INVESTIGATIONS AND COMPLIANCE ASSESSMENTS	A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE

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

30400		INVESTIGATIONS AND COMPLIANCE ASSESSMENTS	A	SA	FD
	-01	**General**	CY+2y	nil	DE
PIB	**-20**	**Investigation case files** (includes assignment notices, privacy breach harm assessment reports, records with stakeholders (e.g., Office of the Information and Privacy Commissioner (OIPC) and Information Security Branch), general incident loss reports, audio files, transcripts, statutory declarations, notifications to affected individuals, closing notes, supporting documentation, advice, and correspondence) (also covers data in the File Management System (FMS)) (arrange by year, then by case number) SO: when investigation is closed or abandoned, and the files are no longer required for research and reference purposes (see note below) 5y: The five year semi-active retention period meets the operational and reference needs of the branch to have access to past investigations. DE: These records have been appraised for destruction because records pertaining to significant investigations are classified under *ARCS* primary 280 and/or by special schedule 102906 (*Executive Records*), which are selectively retained. NOTE: Only a small subset of investigation case files are deemed precedent-setting or of ongoing reference value. To facilitate disposition of routine investigations, investigators will identify the precedent-setting/ongoing reference value files at the time of file closure.	SO	5y	DE
	-30	**Central agency assessments - final** (includes terms of reference, assessment plan, final assessment report, recommendations, and action plan created by assessed ministry) SO: when the following criteria are complete: • for scheduled assessments, when assessment is complete, and three subsequent scheduled assessments have been completed • for ad hoc assessments, when no longer needed for research and reference, plus an additional seven years	SO	nil	SR

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

30400	INVESTIGATIONS AND COMPLIANCE ASSESSMENTS	A	SA	FD
	SR: The government archives will fully retain scheduled assessments because they provide a concise, high-level summary of ministries' overall compliance with legislative requirements in the areas of privacy, access, records management, and information protection/security. Ad hoc assessments will be destroyed.			
-35	**Central agency assessments - development files** (covers records pertaining to the development of central agency assessments) SO: when the corresponding assessment is complete and records are no longer required for research or reference purposes NOTE: See secondary secondary 30400-30 for central agency completed assessments. For the development of ministry self-assessments, see secondary 30400-40.	SO	nil	DE
-40	**Ministry self-assessments** (includes terms of reference, self assessment tool, self-assessment report, client action plan, correspondence, case notes, findings, recommendations, assessment plan, and final assessment report) SO: at the end of the calendar year in which the self-assessment is completed, plus an additional seven years 7y: The seven year semi-active retention period meets the operational and reference needs of the branch to have access to past assessments. DE: Self-assessments have been appraised for destruction because the assessments are routine in nature, consisting simply of a maturity model filled out annually. In many cases, the information contained in a self-assessment is also duplicated in the scheduled assessments, which are fully retained (under secondary 30400-30).	SO+7y	nil	DE

END OF PRIMARY

INFORMATION AND PRIVACY

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (*ORCS*)

SYSTEMS SECTION TABLE OF CONTENTS

SECTION AND TITLE	PAGE NO.
COMMON SYSTEM NOTES	14
FILE MANAGEMENT SYSTEM (FMS)	15

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

SYSTEM SECTION: COMMON SYSTEM NOTES

Retention Schedules for the Systems

The data on the systems is classified under appropriate secondaries in the *ORCS* and in *Administrative Records Classification System* (*ARCS*), as indicated in the following descriptions. The systems themselves are all scheduled as follows:

Active	SO:	The system becomes superseded and obsolete when all data has been migrated to another system or documented elsewhere, or when all applicable retention schedules for the data have expired; see relevant classifications.
Semi-Active	nil:	There is no semi-active retention period assigned to systems.
Final Disposition	DE:	Each system will be destroyed when all data has been migrated to another system performing the same function, schedules covering the data have elapsed, or the data has been preserved elsewhere. For data retention details, see the applicable system overview.

FILE MANAGEMENT SYSTEM (FMS)

SYSTEM OVERVIEW

Creating Agency
Ministry of Citizens' Services
Corporate Information and Records Management Office
Privacy, Compliance and Training Branch
Investigations Unit

System Title
File Management System (FMS)

Purpose
FMS is a web-based, integrated case management system, used by investigators to manage their investigation work flow, document their analysis, and record key facts for future reference; the system also helps the Investigations Unit analyze trends.

FMS is a shared system with the Investigations & Forensics Unit (IFU) of the Information Security Branch, Ministry of Citizens' Services. This system overview only covers data created by the Investigations Unit of Privacy, Compliance and Training Branch. Data created by IFU is covered under the *Information Technology Services ORCS*, schedule 143282.

Information Content
FMS contains the investigator's notes and analysis, information about the incident and the investigative actions taken, contact information for persons involved in the investigation and their relationship to the event, and summary facts and data about the events investigated and the persons involved. It may contain conclusions and recommendations.

FMS was launched in 2013 and contains data ranging from 2011 to present.

Inputs, Processes, and Outputs
Inputs
FMS inputs consist of information that the investigator enters directly in the course of reviewing and analyzing the incident and managing the work flow. Some information may be copied from or summarize information gathered in the course of carrying out the investigation.

Processes
When an investigation is closed, an investigator will indicate in the system if the investigation data is required for research or reference purposes. Investigations designated with this indicated will not be purged from the system. This function does not currently exist in FMS.

Outputs
FMS outputs consist of statistical reports and reports that show the relationships between data elements, investigation narratives, timelines and/or pre-defined reports in the system.

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

FILE MANAGEMENT SYSTEM (FMS)

Classification of Records that Relate to the System

Schedule Code	Secondary No.	Secondary Title	Retention Schedule A	SA	FD
Data in the System					
INFP	30400-20	Investigation case files	SO	5y	DE
Inputs					
INFP	30400-20	Investigation case files	SO	5y	DE
Outputs					
ARCS	400-20	Ministry/agency planning and performance files	SO	2y	DE
INFP	30400-20	Investigation case files	SO	5y	DE
ARCS	440-20	Reports and statistics	CY+1y	nil	DE
Other Related Records					
ARCS	6820-05	Back-up data	SO	nil	DE
ARCS Section 6	see appropriate secondaries	INFORMATION TECHNOLOGY			
102902		Transitory Electronic Data Processing (EDP) Records	SO	nil	DE

Schedule Code Key: *ARCS = Administrative Records Classification System*, schedule 100001
INFP = Information and Privacy ORCS, schedule 194900

END OF OVERVIEW

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

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD

This concordance table is intended as a general guide for transition between the old and new versions of this *ORCS*. The new classifications and retentions are to be applied to all relevant digital and physical operational records, both in the office and in storage. When converting old files to the new *ORCS*, you will need to check file contents to ensure that the recommended replacement secondary is appropriate for that particular file.

NOTE: Superseded secondaries have been deleted from section 1 of the *ORCS*. Superseded/defunct systems have also been deleted from the Systems Overview Section. Details are provided below.

SECTION 1 – INFORMATION AND PRIVACY			
30000	**INFORMATION AND PRIVACY – GENERAL (title unchanged)**		
30000-00	Policies, procedures, and resources - final	This secondary is now the policy and procedures secondary for the entire *ORCS*. SO definition updated. Supersedes: • -00 from all original primaries • 30000-03 Information and privacy information bulletins • 30200-02 Information and privacy policy - approved	**SO/5y/FR** (unchanged)
30000-02	Information and privacy annual reports	Superseded by *ARCS* secondary 400-02 Final annual reports (not covered in an *ORCS*)	Changed from CY+5y/nil/FR to **SO/nil/FR**

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

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30000-03	Information and privacy information bulletins	Superseded by 30000-00 Policies, procedures, and resources - final	Changed from SO/nil/FR to **SO/5y/FR**
30000-04	Information and privacy web sites	Superseded by *ARCS* primary 340	**Varies; see applicable secondaries within *ARCS* primary 340**
30000-05	Tracking spreadsheets and registers	NEW Supersedes 30200-03 Information and privacy policy project tracking Covers all areas of branch activity with regards to tracking.	**SO/nil/DE**
30000-20	Information and privacy report and bulletin development case files	Title changed to Policies, procedures, and resources - development files. SO definition updated. Supersedes secondary 30200-20 Information and privacy policy development case files Records pertaining to the development of information and privacy annual reports are now classified under *ARCS* secondary 400-20 Ministry/agency planning and performance files.	**SO/5y/DE** for development of policies, procedures and resources (unchanged) Development of information and privacy annual reports changed from SO/5y/DE to **SO/2y/DE**
30000-30	Information and privacy project case files	Superseded by secondary 30100-20 Client review and advice case files	Increased from SO/nil/DE to **SO/5y/DE**
30000-40	Information and privacy reference and issue case files	Superseded by secondary 30100-20 Client review and advice case files	Increased from SO/nil/DE to **SO/5y/DE**

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

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30100	**INFORMATION AND PRIVACY ADVISORY SERVICES – title changed from "INFORMATION AND PRIVACY – ADVICE AND COMPLIANCE"**		
30100-00	Policy and procedures	Superseded by secondary 30000-00 Policies, procedures, and resources - final	**SO/5y/FR** (unchanged)
30100-02	Corporate information access request statistical reports	Superseded by secondary 30100-02 in the *Information Access ORCS*, schedule 144018.	Unchanged
30100-03	Privacy breach reporting	Superseded by secondary 30400-20 Investigation case files	Increased from SO/nil/DE to **SO/5y/DE**
30100-04	Foreign demands for disclosure	NEW Supersedes secondary 30100-80 Unauthorized foreign demand for disclosure case files	Changed from CY+5y/nil/DE to **CY+2y/nil/DE**
30100-20	Client review and advice case files	Scope broadened to cover the following: review and advice activities provided by the branch in relation to client developed privacy policies, PIAs, corporate PIAs, integrated program or activity agreements (IPAs), research agreements, information sharing agreements (ISAs), contracts, and privacy protection schedules; provision of support to Ministry Privacy Officers; provision of support to ministries in their interactions with the OIPC; and lastly, liaison with the OIPC. SO definition updated. Supersedes: • 30000-30 Information and privacy project case files • 30000-40 Information and privacy reference and issue case files • 30100-60 Privacy impact assessment (PIA) review case files	**SO/5y/DE** (unchanged)

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

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30100-25	Corporate information access request tracking data files	Superseded by secondary 30100-25 in the *Information Access ORCS,* schedule 144018.	Unchanged
30100-30	Cross-government information access request case files	Superseded by secondary 30100-30 in the *Information Access ORCS,* schedule 144018.	Unchanged
30100-40	Impact analysis of Commissioner's orders or investigations	CLOSED – This function is no longer performed by PCT.	**CY+5y/nil/FR**
30100-50	Information access requests deemed not cross-government	Superseded by secondary to 30100-50 in the *Information Access ORCS,* schedule 144018.	Unchanged
30100-55	Personal information directory summary data files	Superseded by secondary 30100-65 Personal information directories and inventories	**SO/nil/DE** (unchanged)
30100-60	Privacy impact assessment (PIA) review case files	Superseded by secondary 30100-20 Client review and advice case files	Changed from SO/nil/DE to **SO/5y/DE**
30100-65	Personal information directories and inventories	NEW SO definition updated. Supersedes secondary 30100-55 Personal information directory summary data files	**SO/nil/DE**
30100-70	Review of other jurisdiction's issues case files	Superseded by *ARCS* secondary 358-20 Library/topical reference files.	Unchanged

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30100-75	Research unit - reports and development files	NEW CLOSED - This function is no longer performed by PCT. This unit operated from 2006 to 2012, and created records that were not covered by the previous schedule. A new secondary was created to schedule the records, but the status was changed to closed to reflect that records are no longer being created.	**SO/nil/SR**
30100-80	Unauthorized foreign demand for disclosure case files	Superseded by secondary 30100-04 Foreign demands for disclosure	Changed from CY+5y/nil/DE to **CY+2y/nil/DE**
30200	**INFORMATION AND PRIVACY - POLICY DEVELOPMENT (PRIMARY CLOSED – secondaries are superseded as listed below)**		
30200-00	Policy and procedures	Superseded by secondary 30000-00 Policies, procedures, and resources - final	**SO/5y/FR** (unchanged)
30200-01	General	Superseded by secondary 30000-01 General	Unchanged
30200-02	Information and privacy policy - approved	Superseded by secondary 30000-00 Policies, procedures, and resources - final	**SO/5y/FR** (unchanged)
30200-03	Information and privacy policy project tracking	Superseded by secondary 30000-05 Tracking spreadsheets and registers	**SO/nil/DE** (unchanged)
30200-20	Information and privacy policy development case files	Superseded by secondary 30000-20 Policies, procedures, and resources - development files	**SO/5y/DE** (unchanged)

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

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30300	**INFORMATION AND PRIVACY – TRAINING** **(PRIMARY CLOSED – secondaries are superseded as listed below)**		
30300-00	Policy and procedures	Superseded by secondary 30000-00 Policies, procedures, and resources - final	**SO/5y/FR** (unchanged)
30300-01	General	Superseded by *ARCS* secondary 1735-01	Changed from CY+2y/nil/DE to **CY+1y/nil/DE**
30300-02	Information and privacy proof of certification - electronic	CLOSED – This secondary was never used by client	**N/A**
30300-20	Information and privacy training case files	Superseded by *ARCS* secondary 1735-05	Changed from SO/5y/DE to **SO/2y/SR**
30400	**INVESTIGATIONS AND COMPLIANCE AUDITS (NEW primary)**		
30400-01	General	NEW	**CY+2y/nil/DE**
30400-20	Investigation case files	NEW Supersedes secondary 30100-03 Privacy breach reporting	**SO/5y/DE**
30400-30	Central agency audits - final	NEW	**SO/nil/SR**
30400-35	Central agency audit - development files	NEW	**SO/nil/DE**

For a full listing of the codes and acronyms used above, see Key to *ARCS/ORCS* Codes and Acronyms

APPENDIX A: Summary of Amendments to the *Information and Privacy ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
30400-40	Ministry self-assessment audits	NEW	**SO+7y/nil/DE**
SYSTEMS SECTION			
N/A	Corporate Request Tracking System (CRTS)	Superseded by the *Information Access ORCS*, schedule 144018.	**N/A**
N/A	Personal Information Directory (PID) Database	Database is defunct.	**N/A**
N/A	Information and Privacy internet web site	Superseded by *ARCS* primary 340. Web Site Overview no longer required.	**N/A**
N/A	Information and Privacy internet web site	Superseded by *ARCS* primary 340. Web Site Overview no longer required.	**N/A**