

Records Management Policy

University Policy No: IM7700

Classification: Information Management

Approving Authority: Board of Governors

Effective Date: November 2022

Supersedes: July 2018

Last Editorial Change:

Mandated Review: November 2029

Associated Procedures:

[Procedures for the Management of University Records](#)

[Procedures for the Access to and Correction of Information](#)

[Procedures for the Secure Destruction and Deletion of University Records and Information](#)

[Procedures for the Imaging of University Records](#)

PURPOSE

1.00 The purpose of this policy is to:

- ensure that university Records are created, used, disposed of and preserved in a systematic manner, compliant with relevant legislation;
- ensure that Access is provided to Records in compliance with the [Freedom of Information and Protection of Privacy Act](#) (FIPPA); and
- define authorities, responsibilities, and accountabilities for Records Management.

DEFINITIONS

2.00 **Access** includes both disclosure of Records under FIPPA as a result of a request, and routine release of Records that contain information that is available to the public or to an individual.

3.00 **Administrative Authority** means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, Executive Directors, Chief Information Officer, and other Unit heads.

4.00 **Disposition** means disposal of Records no longer needed for day-to-day operations by a Unit, through destruction, secure destruction, or transfer to the university archives.

5.00 **Records** means documents created or received, and retained in the day-to-day operations of business. These include, but are not limited to, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

6.00 **Records Management** means the application of systematic control to the creation, use, maintenance, storage, retrieval, disposition, and preservation of all forms of recorded information produced by the university in the conduct of its operations.

- 7.00 **Unit** means academic or administrative areas at the university, including but not limited to: faculties, departments, divisions, offices, schools and centres.

JURISDICTION/SCOPE

- 8.00 This policy applies to all Records in the custody or under the control of the university and to the management of Records by all Units. It does not apply to academic instructional material or research data.

POLICY

- 9.00 The university will manage Records in order to meet its business, fiscal, and legal requirements.

Roles and Responsibilities

- 10.00 Consistent with section 64(1) of the [University Act](#), the University Secretary is responsible for the oversight of records management at the university.
- 11.00 The University Archivist is responsible for:
- maintenance of the university's Records Management program, including the university-wide Records classification, retention and Disposition plan;
 - developing Records Management policy and procedures, and providing standards and guidelines to assist Units in the implementation of Records Management;
 - providing Records Management training and advisory services to Units; and
 - providing Access to university Records selected for permanent retention.
- 11.01 The University Archivist reports to the University Secretary and the University Librarian for these purposes.
- 11.02 University Archives staff will assist Units with Records Management.
- 12.00 Administrative Authorities are responsible for making reasonable efforts to ensure that:
- Records in their Unit are managed according to this policy and related procedures;
 - employees in their Unit manage Records according to this policy and related procedures; and
 - Records containing personal or confidential information are protected from unauthorized Access and disclosure, in accordance with the [Protection of Privacy Policy \(GV0235\)](#) and the [Information Security Policy \(IM7800\)](#) and related procedures.
- 13.00 When leaving a position, a university employee must ensure that university Records are left in the custody or under the control of the university.
- 14.00 The Coordinating Committee for Privacy, Records Management, and Personal Information Security has oversight on policies, procedures, strategies and guidelines needed to:
- establish and maintain a university-wide framework to manage university Records;
 - meet the university's business, legal and fiscal requirements; and
 - ensure preservation of the university's corporate memory through selecting Records for permanent retention.

- 15.00 Any Records that are in the custody or under the control of the university as a result of the terms of a contract must be managed according to this policy, the [Protection of Privacy Policy \(GV0235\)](#), and the [Information Security Policy \(IM7800\)](#).

Creation

- 16.00 Records are created by Units in order to carry out the university's business and perform necessary transactions. Units are expected to use the university-wide classification plan to classify Records, thereby enabling effective retention and Disposition.

Access

- 17.00 The university is committed to providing Access through routine release of Records where possible.
- 18.00 Access to Records not covered by routine release is governed by the university's [Procedures for the Access to and Correction of Information](#).

Disposition

- 19.00 Records scheduled for Disposition containing personal or confidential information and identified as having no long-term value must be destroyed in a secure and permanent manner.
- 20.00 Records that will be kept permanently by the university will be held by and preserved for Access as determined by the University Archivist.
- 21.00 When the university retains an external organization to undertake work on its behalf, and that work involves the Disposition of Records, including those containing Personal Information, the university will enter into an agreement with that organization that requires the organization to return or destroy those Records in a secure and permanent manner.
- 22.00 Records scheduled for Disposition (including Transitory records) must not be Disposed of when such Records are:
- identified in current or pending litigation;
 - responsive to a current request made under FIPPA;
 - the subject of an audit; or
 - identified in quasi-judicial and legal proceedings.

Authorities and Officers

- i) Approving Authority: Board of Governors
- ii) Designated Executive Officer: President
- iii) Procedural Authorities: *Refer to individual procedures*
- iv) Procedural Officers: *Refer to individual procedures*

Relevant Legislation

- [Freedom of Information and Protection of Privacy Act](#)
- [University Act](#)
- [Limitations Act](#)

Related Policies and Documents

Associated Records Management Procedures

- [Procedures for the Management of University Records](#)
- [Procedures for the Access to and Correction of Information](#)
- [Procedures for the Secure Destruction and Deletion of University Records and Information](#)
- [Procedures for the Imaging of University Records](#)

[Protection of Privacy Policy \(GV0235\) and associated Procedures](#)

- [Procedures for the Disclosure of Personal Information in Emergency or Compelling Circumstances](#)
- [Procedures for the Management of University Surveillance Systems](#)
- [Procedures for Responding to a Privacy Incident or Privacy Breach](#)
- [Privacy Protection Schedule](#)

[Information Security Policy \(IM7800\)](#)

Procedures for the Management of University Records

Procedural Authority: University Secretary
Procedural Officer: University Archivist

Effective Date: December 2023
Supersedes: December 2022
Last Editorial Change:

Parent Policy: [Records Management Policy \(IM7700\)](#)

PURPOSE

- 1.00 The purposes of these procedures are to:
- assist Units in making reasonable efforts to create, use, maintain and dispose of university Records, whether in paper, electronic, audio-visual or other format, in a manner that:
 - complies with the [Freedom of Information and Protection of Privacy Act](#) (FIPPA) and other pertinent legislation; and
 - is consistent with the university's [Records Management \(IM7700\)](#), [Protection of Privacy \(GV0235\)](#) and [Information Security \(IM7800\)](#) policies and the Directory of Records;
 - regulate the Disposition of university Records in all formats, whether paper, electronic or other; and
 - describe the process for approving new or revising the existing functional classification structure, Series, and Retention Rules contained in the Directory of Records.

DEFINITIONS

- 2.00 The definitions contained in the university's Records Management policy (IM7700) apply to these procedures.
- 3.00 **Active Records** are Records that are maintained and used by a Unit or Units for current business.
- 4.00 **Authorized Disposition** means a Disposition of Inactive Records carried out with the approval of the University Archivist and the Unit's Administrative Authority (see also [Disposition](#) definition in IM7700).
- 5.00 **Directory of Records (DOR)** is the university-wide classification, retention and Disposition plan that arranges Records according to the functions of the university and identifies these functional groups by a block-numeric system for the efficient access, retrieval, and Disposition of Records.
- 6.00 **Inactive Records** are Records that are no longer needed for current business.

- 7.00 **Primary Office** is an office or offices responsible for keeping the original and/or official versions of Records, and responsible for carrying out the approved Disposition of such Records.
- 8.00 **Retention Rules** are the instructions in the Directory of Records to Primary and Secondary Offices regarding the length of time for which records should be kept.
- 9.00 **Secondary Office** is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.
- 10.00 **Semi-active Records** are Records that are required infrequently for current business; they are used for reference or required to comply with legislated retention. Semi-active records are an opportunity to make use of off-site or other less expensive secondary storage.
- 11.00 **Series** is a group of Records relating to a particular function, resulting from the same activity, or having a particular form. Within the Directory of Records functions, Records are arranged in Series.
- 12.00 **Transitory Records** are Records of temporary usefulness, required only for a limited period of time for the completion of a routine action or the preparation of an ongoing Record. Transitory Records do not include those Records required to meet statutory obligations, or to sustain administrative or operational functions (i.e. subject to a retention rule). Transitory Records may include drafts, notes, calculations, and superseded documents.
- 13.00 **Vital Records** are Records that are necessary to re-establish or continue the business of the university in the event of a disaster, including those that are necessary to re-create the university's legal and financial position, necessary to preserve the rights of the university, its students and employees, and others associated with the university.

SCOPE

- 14.00 These procedures apply to all Units and to university Records held by external organizations that undertake work with the university.

PROCEDURES

Classifying and Managing Active and Semi-Active Records

- 15.00 Units should consult the Directory of Records in order to classify university Records for which they are responsible and identify the:
- function to which the file or single document relates;
 - appropriate functional section from the Directory of Records (e.g., Financial Management, Human Resources, etc.);
 - appropriate series by considering the action, content and source of the document; and
 - primary and secondary number.

Units should consult university archives staff for Unit-specific advice on records classification.

- 16.00 Unit staff are expected to identify whether the Unit has any Vital Records and set procedures to give Vital Records the protection they require in case of disaster (the Directory of Records identifies Vital Records). The Primary Office, as identified on the Retention Rules, is responsible for ensuring the protection of Vital Records.
- 17.00 Unit staff are expected to identify the classification levels of the information and Records in the Unit for security purposes in accordance with the university's Information Security Classification Procedures.
- 18.00 Units should destroy or delete Transitory Records from files when such documents are no longer needed for reference.
 - 18.01 Units should destroy or delete non-record materials when they are no longer required for reference by a Unit. Non-record materials include but are not limited to:
 - published material such as books, pamphlets, circulars, newsletters, brochures, catalogues, and other information created for informational or reference purposes; and
 - excess stock of forms.

Storage of Semi-Active Records

- 19.00 Units are responsible for storage of their own Semi-Active Records.
 - 19.01 The University Archives does not provide storage for Semi-Active Records.
 - 19.02 Units may make use of private, off-site storage of these records. Consult with the Archives for service providers.

Disposition of Inactive Records

- 20.00 Unit offices identified as Primary Offices for particular Record Series are responsible for conducting Authorized Dispositions of Inactive Records (whether in paper, electronic, audio-visual or other format) in accordance with the Directory of Records.
 - 20.01 Units are responsible for determining on an annual basis what Records should be disposed of by consulting the Retention Rules of the Series that pertain to their activities.
 - In consultation with Archives, use the Approved Retention Rule form for destruction of Records.
 - 20.02 Some Series and sections in the Directory of Records have Retention Rules which are not yet approved. Incomplete retention rules do not preclude Authorized Disposition. In these cases, contact the University Archives for retention advice.

20.03 Refer to the university's [Procedures for the Secure Destruction and Deletion of University Records and Information](#) for direction regarding acceptable forms of secure Records destruction. The method for Secure Destruction must be appropriate for the medium on which information is stored.

21.00 Unit offices not identified as Primary Offices for particular Record Series may destroy or delete such Records as specified for "other offices" in the approved Retention Rules, or when they are no longer useful to the Secondary Office. There is no requirement to conduct an Authorized Disposition.

Transfer of Records to University Archives

22.00 Records transferred to the university archives are deemed Inactive Records that are either:

- specified by the Retention Rules for transfer to the university archives; or
- identified as having long-term legal, administrative or historical value by the University Archivist (or designate), in consultation with the respective Unit staff.

23.00 When a Unit seeks to transfer Records to the University Archives, it must contact the:

- University Archives before sending any Records to ensure that only Records with archival value are transferred; and
- University Archivist directly if the Records intended for transfer are in electronic form only.

23.01 The University Archivist or Associate Archivist will provide further direction regarding the transfer of Records to the university archives.

Access to Records Transferred to the University Archives

24.00 Primary Offices may access their archival Records transferred to the university archives without restriction. Other offices may, on a need-to-know basis, access records on request to University Archives.

25.00 University Records transferred to the archives are arranged and described according to archival principles, are listed in publicly available databases, and are available for Access to the public unless Access is restricted by FIPPA.

Approval of changes to the Directory of Records

26.00 As a part of the ongoing management of university Records, the University Archivist will review the Directory of Records' functional classification structure, Series, and Retention Rules in light of changes to university functions, organizational structure, Unit responsibilities, technologies and relevant legislation.

27.00 Following annual consultation with the Privacy, Records Management and Personal Information Security Co-ordinating Committee, Archives staff will work with Primary Offices to identify DOR sections for review.

- 28.00 Following agreement between Archives and Primary Office staff that the new or revised functional classification structure, Series, and Retention Rules reflect the required or desired changes, the draft revisions will be presented for approval to the Administrative Authority for the Primary Office.
- 28.01 If the draft revisions require further consultation, Archives and Primary Office staff will work together to incorporate desired changes.
- 29.00 Following approval of new or revised functional classification structure, Series, and Retention Rules by the Administrative Authority for the Primary Office, the draft changes will be presented to the DOR Sub-committee of the Privacy, Records Management and Personal Information Security Co-ordinating Committee for review.
- 29.01 If the DOR Sub-committee determines that the new or revised functional classification structure, Series, and Retention Rules presented need further revisions, Archives and Primary Office staff will work together to incorporate desired changes.
- 30.00 The DOR Sub-committee will recommend the new or revised functional classification structure, Series, and Retention Rules through the University Archivist to the University Secretary for approval and signature.
- 31.00 Following the approval of the University Secretary, the relevant sections of the Directory of Records will be updated in the official version.
- 32.00 The official version of the Directory of Records is the on-line database.
- 33.00 The original approved and signed functional classification structure, Series, and Retention Rules will be kept in hard-copy in the University Archives.
- 34.00 Editorial changes to DOR that do not affect Records classifications or retention periods may be made upon written recommendation from the Administrative Authority for the Primary Office and the University Archivist to the University Secretary.

RELEVANT LEGISLATION

- [*Freedom of Information and Protection of Privacy Act*](#)
- [*Evidence Act \(B.C.\)*](#)
- Federal and Provincial legislation pertinent to specific Units and Records

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy

- [Procedures for the Management of Personal Information](#)

Records Management Policy

- [Procedures for Access to and Correction of Information](#)
- [Procedures for the Secure Destruction and Deletion of University Records and Information](#)
- [Procedures for the Imaging of University Records](#)

Information Security Policy

- [University Information Security Classification Procedures](#)
- [Records Disposition Application – for records *without* an Approved Retention Rule](#)
- [Records Disposition Application – for records *with* an Approved Retention Rule](#)
- [Transitory Records](#)

Procedures for Access to and Correction of Information

Procedural Authority: General Counsel
Procedural Officer: University Archivist; Chief
Privacy Officer

Effective Date: August 2023
Supersedes: June 2017

Last Editorial Change:

Parent Policy: [Records Management Policy \(IM7700\)](#)

PURPOSE

- 1.00 The purpose of these procedures is to set out how the university will manage:
- Freedom of Information access requests;
 - requests for correction of Personal Information in the university's custody or control;
 - requests to access Records in the University Archives and Special Collections;

in accordance with the [Freedom of Information and Protection of Privacy Act](#) (FIPPA), and where appropriate, the [Personal Information Protection Act](#).

DEFINITIONS

- 2.00 The definitions contained within the university's [Records Management \(IM7700\)](#) and [Protection of Privacy \(GV0235\)](#) policies apply to these procedures.

PROCEDURES

RESPONDING TO REQUESTS

- 3.00 When an individual contacts a Unit seeking Access to their Personal Information or Access to a Record in the custody or under the control of the university, the Unit's Administrative Authority (or designate) will assess whether the individual is seeking Access to:
- (a) their Personal Information (e.g., the individual's file or a specific Record pertaining to that individual); or
 - (b) a university Record on a particular subject.
- 3.01 If the individual is seeking access to their Personal Information, after confirming the individual's identity, the Unit may disclose the information to the individual if that information is routinely disclosed by the Unit in response to such requests.

- 3.02 If the individual is seeking Access to university Records on a particular subject that do not include the Personal Information of the applicant, the Unit may disclose the information to the individual if that information is routinely disclosed by the Unit in response to such requests.
- 3.02.01 If the information or Record sought is publicly available on the university's website, the Unit will proactively assist the individual in finding such information or Record.
- 3.03 If the individual is seeking access to a Record(s) that contains information about other individuals, was created with an expectation of confidentiality, or is a type of Record that contains information that the Unit does not routinely disclose upon request, the request must be promptly transferred by the Unit to the Privacy and Access to Information Office to be processed as a Freedom of Information access request .
- 4.00 After an access request is transferred by a Unit to the Privacy and Access to Information Office, all communication with the applicant for the purpose of the access request will be handled by that office.
- 5.00 Records or information that are responsive to an access request must not be destroyed after a request has been received.
- 6.00 The retention rule for GV260-30 [Freedom of Information requests](#) in the Directory of Records applies to a Unit's Records created for the purpose of processing and responding to a Freedom of Information access request .
- 7.00 Employees must treat Freedom of Information access requests as confidential, including the applicant's identity, contact details, and role. Information about access requests is to be used or shared only to the extent necessary to respond to the access request.
- 8.00 Employees shall not ask an applicant the reason(s) for which they have submitted an access request.
- 8.01 If an applicant voluntarily shares this information with an employee, it should not be used or disclosed to anyone else at the university except in emergency circumstances or for the purpose of obtaining legal advice.

Receiving a Freedom of Information access request – Privacy and Access to Information Office

- 9.00 In accordance with FIPPA, access requests must be made in writing. If an applicant has not made their request in writing, the Privacy and Access to Information Office shall ask the individual to make a written request in one of the following ways:
- (a) by completing and submitting the Freedom of Information Request form available on the Privacy and Access to Information Office's website; or

(b) by submitting a written request that specifies the Records the applicant is seeking and includes the applicant's contact information.

- 10.00 If an access request is for Records containing the applicant's Personal Information, then the applicant must provide proof of their identity, by providing government-issued photo identification matching the address and signature on the access request.
- 11.00 If an access request is for Records containing a third party's Personal Information, then the applicant must submit proof of consent by the third party, in a manner that complies with the FIPPA regulation, and confirms the identity of the third party.

Processing a Freedom of Information access request – Unit Responsibilities

- 12.00 Upon receiving an access request, the Privacy and Access to Information Office will send the relevant Unit(s) a Call for Records requiring them to provide Records responsive to that request before a given deadline.
 - 12.01 The Unit's Administrative Authority (or designate) will appoint a Unit liaison to coordinate with the Privacy and Access to Information Office for the production and delivery of the Unit Records identified as responsive.
 - 12.02 In a search for and production of Records, Units must follow the instructions in the Call for Records.
- 13.00 The Privacy and Access to Information Office will work closely with Unit(s) asked to search, locate, and produce responsive Records by doing necessary follow up, answering enquiries, and by providing one-to-one or team access training, when requested by Unit(s) processing an access request.
- 14.00 The university may consult with third parties in accordance with FIPPA if Records contain information about such parties. The Privacy and Access to Information Office will determine and manage consultations with third parties. Units may be asked to provide third parties' contact details for this purpose.
- 15.00 The university may charge fees for access requests, in accordance with FIPPA. The General Counsel (or delegate) determines whether to apply these fees.
 - 15.01 When a fee is applied to an access request, the Privacy and Access to Information Office will ask Unit(s) to estimate the number of hours required to locate, retrieve and produce the Records, and provide an estimate of the number of Records initially identified as responsive.

CORRECTION OF PERSONAL INFORMATION

- 16.00 An individual who believes there is an error or omission in their Personal Information in the custody or under the control of the university may request that the university correct that information.

- 17.00 When an individual contacts a Unit to request a correction to their personal information, Unit staff as authorized by the Unit's Administrative Authority will assess if the individual is able to make the change through the university's online self-service portal. Personal Information that may be changed through the self-service portal includes: phone numbers, postal addresses, additional e-mail addresses, and emergency contact information.
- 17.01 If the information cannot be changed by the individual through the online self-service portal, the Unit will inform the individual of the steps required to correct their personal information, including the provision of appropriate documentation.
- 18.00 If the steps set out in section 17.00 do not resolve the matter, the Unit will ask the individual to make their correction request by one of the following means:
- (a) by completing and submitting the correction request form available on the Privacy and Access to Information website;
 - (b) by submitting a written request to the Privacy and Access to Information Office that specifies the correction they are seeking, the location of the information (i.e., Unit responsible), a description of the information, the reasons for the correction and the individual's contact address; or
 - (c) by procedures established by the Registrar.
- 19.00 The university will process the request and determine if the correction will be made, and the Privacy and Access to Information Office or the Office of the Registrar will notify the individual in writing.
- 20.00 If the request is approved, the appropriate Unit will replace the information with the correct information in a timely manner.
- 21.00 If the request is denied, the appropriate Unit will annotate the information with the correction requested, in accordance with FIPPA.
- 22.00 Evaluative comments or assessments and opinions about individuals may, on request, be annotated but not corrected.
- 23.00 If the General Counsel determines that a correction will be made to an individual's information, any other public body or any third-party to whom that information has been disclosed during the one-year period before the correction was requested must be notified of the correction.

ACCESS TO RECORDS IN SPECIAL COLLECTIONS AND THE UNIVERSITY ARCHIVES

- 24.00 In accordance with FIPPA, the University Archives may disclose Personal Information in university Records for archival or historical purposes in certain circumstances.

- 24.01 Archival descriptions of university Records, also known as finding aids, will specify whether Records must be reviewed for any exceptions to disclosure under FIPPA prior to use of the Records.
- 25.00 The [*Personal Information Protection Act*](#) (PIPA) may apply to records donated by organizations, and permits disclosure for archival or historical purposes in certain circumstances.

The Archivist responsible will review records for Personal Information prior to Access and apply PIPA including, if necessary, the implementation of a research agreement regarding disclosure.

Archives Access Procedures

- 26.00 To access records in the University Archives, an individual should identify the accession number and file titles of the Records that are required (located in the finding aid).

26.01 The Archivist responsible will review the Records.

- (a) If Records containing information that may be subject to any exceptions to disclosure under FIPPA can reasonably be removed from the file(s), the remainder of the file(s) will be provided to the individual requesting Access, as mutually agreed.
- (b) If an individual requests Access to information that may be subject to any exceptions to disclosure under FIPPA, the Archivist responsible will assess whether the individual is seeking Access to their Personal Information (e.g. the individual's file or a specific Record pertaining to that individual), or a university Record on a particular subject, and will ask the individual to make an access request to the Privacy and Access to Information Office.
- (c) If the individual is seeking access to their Personal Information, after confirming the individual's identity, the Archives may disclose the information to the individual if that information is routinely disclosed by the Archives in response to such requests.
If the individual is seeking Access to university Records on a particular subject that do not include the Personal Information of the applicant or other information subject to exceptions to disclosure under FIPPA, the Archives may disclose the information to the individual if that information is routinely disclosed by the Archives in response to such requests.
- (d) If the information or Record sought is publicly available on the university's website, the Archives will proactively assist the individual in finding such information or Record.

Research Agreements

- 27.00 In accordance with FIPPA, the university may allow access to Records containing Personal Information for statistical and research use through the signing of a research agreement between the university and an applicant governing the conditions of Access and use.

RELEVANT LEGISLATION

[*Freedom of Information and Protection of Privacy Act*](#)
[*Personal Information Protection Act*](#)

RELATED POLICIES AND DOCUMENTS

[Protection of Privacy Policy \(GV0235\)](#)

- Procedures for the Management of Personal Information

[Records Management Policy \(IM7700\)](#)

- Procedures for the Management of University Records

[Information Security Policy \(IM7800\)](#)

- University Information Security Classification Procedures

Procedures for the Secure Destruction and Deletion of University Records and Information

Procedural Authority: University Secretary,
Vice-President Finance & Operations
Procedural Officers: University Archivist and
Chief Information Officer

Effective Date: February 2023
Supersedes: November 2014
Last Editorial Change:

Parent Policies: [Records Management Policy \(IM7700\)](#)
[Information Security Policy \(IM7800\)](#)

PURPOSE

- 1.00 The purpose of these procedures is to protect Records and information in the custody or under the control of the university from unauthorized use or disclosure by informing university employees of:
 - 1.01 How to conduct the physical destruction of paper Records and electronic devices containing information that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction; and
 - 1.02 How to conduct deletion of information in electronic form that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction.

DEFINITIONS

- 2.00 The definitions contained within the university's [Records Management \(IM7700\)](#) and [Information Security \(IM7800\)](#) policies apply to these procedures.
- 3.00 **Primary Office** is an office or offices responsible for keeping the original and/or official versions of Records. **Secondary Office** is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.
- 4.00 **Secure Destruction** means permanent physical destruction of paper records and electronic devices, rendering unreadable or unrecoverable the information they contain.
- 5.00 **Deletion** means removal of information from electronic devices and storage media.

- 5.01 **Routine Deletion** means removal or erasure of information from electronic devices and storage media by marking information as deleted. The information still exists, making data recovery possible unless the information is securely deleted or overwritten.
- 5.02 **Secure Deletion** means the process of deliberately, permanently, and irreversibly removing or erasing information from electronic devices and storage media. Secure Deletion overwrites all addressable locations with a character, its complement, then a random character, and verifies. Where supported by the storage media, a firmware-based secure erase can be triggered to purge all data rendering recovery infeasible. If you require assistance, contact the [Computer Help Desk](#) to arrange for secure deletion of devices and storage media.
- 6.00 **Sanitization** is a process to render access to target data (the data subject to the sanitization technique) on the device or media either effectively inaccessible (but potentially recoverable through data recovery techniques) or effectively irrecoverable. Routine Deletion, Secure Deletion, and Secure Destruction are actions that can be taken to sanitize electronic devices and storage media.

SCOPE

- 7.00 These procedures apply to the following actions taken after the decision to dispose of Records and information consistent with Directory of Records (DOR) retention rules has been made:
- 7.01 The physical destruction of information, whether in paper, electronic, audio-visual or other format. This includes computers and other electronic devices and storage media (e.g. mobile phones); see section 18 below for further examples; and
- 7.02 The Deletion or Sanitization of information in electronic form.

Note that these procedures do not apply where the retention rule calls for the transfer of the record to the Archives. In this circumstance, contact the University Archives.

PROCEDURES

- 8.00 The method for Secure Destruction, Deletion, or Sanitization must be appropriate for the medium on which the information is stored.
- Security Classification
- 9.00 Units are expected to refer to the security classification level of the information and Records prior to their destruction to assist in determining an appropriate destruction method. (See the [Information Security Policy](#).)

Authorization for Secure Destruction and Secure Deletion

10.00 Unit offices identified as Primary Offices for a particular Records classification are responsible for obtaining authorization for Disposition from the University Archives prior to Secure Destruction or Secure Deletion in accordance with the university's [Procedures for the Management of University Records](#) and the Directory of Records. See the [Records Management website](#) for authorization forms.

10.01 Unit offices identified as Secondary Offices for a particular Record series may securely destroy or delete Records past their retention period without authorization from the University Archives.

10.02 Units are encouraged to consult the University Archives for specific guidance on Records Disposition, including Secure Destruction or Secure Deletion if they are not already familiar with the Disposition process.

Secure Destruction of Paper-Based Information

11.00 Records containing Highly-confidential, Confidential, and Internal information are to be shredded in a secure manner; Records containing public information may be recycled.

11.01 Records containing Highly-confidential information (see [Information Security Procedures](#)) should be shredded by a staff member of the Unit that holds the records, or on campus ("onsite") by an external supplier. Records containing Confidential or Internal information may be shredded off campus ("offsite") by an external supplier, or onsite by an external supplier or by a staff member of the Unit that holds the records.

Information Security Level	Highly-Confidential	Confidential	Internal	Public
Destruction, Paper Records	Onsite shredding	Offsite shredding (Onsite optional)	Offsite shredding (Onsite optional)	Recycle

12.00 Units should use the university's preferred external suppliers for shredding services. For supplier names, information on engaging them, and negotiated pricing, see the [Purchasing Services website](#) (requires NetLink login).

12.01 If a Unit does not wish to use the preferred external suppliers for shredding services, the following conditions must be met:

- The external supplier must be NAID certified
- The service is selected in accordance with the [Purchasing Policy \(FM5105\)](#).

13.00 Units may consider the appropriateness of a Unit staff member supervising shredding by an external supplier, but this is not required.

- 14.00 Small quantities of paper Records may be shredded by individual Units. Contact Purchasing Services for recommended shredder models if necessary.
- If a Unit uses its own shredders, the Records must be shredded in a secure manner; secure methods include shredding into strips that are a maximum of one centimetre wide, cross-cut shredding, re-shredding or mixing shredded Records to ensure that information cannot be reconstructed.
 - For Records with Confidential or Highly-confidential information, cross-cut shredding or re-shredding is recommended.
 - If such Records are not cross-cut shredded or re-shredded, the shredded Records should be mixed to ensure information cannot be reconstituted.

If a staff member of a Unit is uncertain about the security classification of the information or Record, the staff member shall use the destruction method for the higher level. Contact the Records Management Archivist with questions.

- 15.00 Records awaiting Secure Destruction must be kept in a secure manner (i.e. locked cabinet, controlled access area, secure supplier's console, or sealed boxes in a locked room).

Electronic Device or Storage Media Sanitization

- 16.00 The approach for handling electronic devices and storage media after use is dependent on whether the devices or media are being repurposed for university use or are no longer required for use, and whether they are owned by the university.
- 17.00 Electronic devices and storage media that have been loaned to or leased by the university such as multi-function devices must have all data on the device Sanitized in a manner that renders it effectively inaccessible.
- 17.01 Electronic devices and storage media that will be repurposed for university use that contain information classified as Confidential or Highly-confidential must be Sanitized using a method that erases data by overwriting the information.
- 18.00 Electronic devices and storage media purchased with university funds or funds administered through the university, and that are repurposed for university use, must have information Sanitized prior to being repurposed.
- 18.01 Electronic devices and storage media that will be repurposed for university use should have all data on the device Routinely Deleted in a manner that renders it effectively inaccessible unless the information is Confidential or Highly-confidential in which case all data on the device must be Securely Deleted.
- 19.00 Electronic devices and storage media purchased with university funds (including Professional Development funds) or funds administered through the university, that are not repurposed for university use, must undergo secure physical destruction when no longer required by a Unit or employee, whether or not they are known to store Internal, Confidential, or Highly-confidential information.

- 19.01 Units must use the central secure physical destruction program provided by University Systems and Purchasing Services. Electronic devices and media requiring secure physical destruction include, but are not limited to: hard drives, solid state storage, flash media, USB thumb drives, optical discs, floppy disks, computer tapes, audio and video storage devices, personal digital assistants, smartphones, tablets, and cellphones. Contact the [Computer Help Desk](#) to arrange for Secure Destruction of electronic devices and storage media.
- 19.02 If the electronic device or storage media was encrypted in accordance with the university's [information security standards](#), the device may be Sanitized using a method that erases data by overwriting the data multiple times instead of secure destruction.
- 19.03 Supervisors who are assessing employee requests to purchase ("buy back") devices purchased with professional development funds (as permitted under policies HR6400, HR6410, and HR6420) must assess whether secure physical destruction is required instead. For assistance, consult with University Systems by contacting the Computer Help Desk.
- 20.00 Electronic Devices or Storage Media that are covered by a manufacturer's warranty may be returned to the manufacturer for warranty repair or replacement if the device has been encrypted in accordance with the university's [information security standards](#). Contact the Computer Help Desk for information on this service or visit <http://www.uvic.ca/secureyourdata>
- Cloud Storage Sanitization
- 21.00 Information that has been provided to Cloud Service Providers must be Sanitized upon termination of the agreement with the Cloud Service Provider per the terms of the agreement.
- 22.00 Sanitization for Cloud Services normally means requesting that information is purged or destroyed and confirmed by a Certificate of Sanitization that affirms the information cannot be recovered (see NIST 800-88, Appendix G for a sample).

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- [Procedures for Responding to Privacy Incidents or Privacy Breach](#)

Records Management Policy (IM7700)

- [Procedures for Access to and Correction of Information](#)
- [Procedures for the Management of University Records](#)
- [Procedures for the Imaging of University Records](#)

Information Security Policy (IM7800)

- [University Information Security Classification Procedures](#)
- [Procedures for Responding to an Information Security Breach](#)

- [NIST SP 800-88](#)
- [NAID](#) certification

RESPONSIBLE OFFICES

Information Security Office
University Archives

Procedures for the Imaging of University Records

Procedural Authority: University Secretary
Procedural Officer: University Archivist

Effective Date: October 2017
Supersedes: **NEW**
Last Editorial Change: August 2023

Parent Policy: [Records Management Policy \(IM7700\)](#)

PURPOSE

- 1.00 The purpose of these procedures is to ensure that digital Imaging Programs will copy source records accurately and reliably, and follow applicable standards and legislation in order to produce Imaged Records that are as credible as their Source Records after the Source Records are disposed of. This will result in Imaging Programs that can dispose of the Source Records once they have been Imaged and all control procedures followed.
- 2.00 These procedures have been drafted to conform to the latest version of the Canadian General Standard Board's *Microfilm and Electronic Images as Documentary Evidence* standard and *Electronic Records as Documentary Evidence* standard, and other applicable standards of evidence as determined by legislation and case law. An Imaging Program that complies with these procedures will also comply with the applicable evidentiary standards.

DEFINITIONS

- 3.00 The definitions contained in the university's Records Management policy (IM7700) apply to these procedures.
- 4.00 **Image** is the digital representation of a Source Record that can be used to generate an intelligible reproduction of that Record, or the reproduction itself, where:
 - (a) the reproduction is made with the intention of standing in place of the Source Record;
 - (b) the interpretation of the reproduction, for the purposes for which it is being used, yields the same information as the Source Record; and
 - (c) the limitations of the reproduction (e.g., resolution, tonal or hues) are well-defined and do not obscure significant details.

The Source Record may be subject to disposal for the purpose of constituting the Image as the permanent Record. (CAN/CGSB-72.11-93, 3.21)

- 5.00 **Imaging Program** is an authorized activity of a university Unit that follows strict control guidelines to achieve efficiency in its business operations through the digital capture, storage, retrieval and disposition of Images. This may also include the confidential disposal of Source Records.

- 6.00 **Evidence** is the body of testimony, documentation and physical objects that will be “admitted into evidence” by a court or tribunal as a proper source for determining facts and making decisions.
- 7.00 **Source Record(s)** is the original document(s) or copies thereof that have the same force as the original, used to produce Images.
- 8.00 **Accuracy** is the degree to which Records and Images are precise, correct, truthful, and free of error or distortion.
- 9.00 **Reliability** is the trustworthiness of a Record as a statement of fact, based on the completeness of the Record's form and the degree of control exercised on the process of its creation.

SCOPE

- 10.00 These procedures do not apply to convenience Imaging Programs where Source Records are retained.
- 11.00 Existing Imaging Programs where the Source Records have been retained but where the Unit would like to dispose of the Source Records will be able to do so with proof of the accuracy of the Images and by demonstrating the Unit's history of successful reliance on those Images.
- 12.00 These procedures will not apply to new digital business processes where the scope of the records is limited ([see Appendix 1](#)).

PROCEDURES

- 13.00 Units proposing to initiate an Imaging Program must seek and obtain approval as specified in these procedures.
- 13.01 A Unit proposing to initiate an Imaging Program will obtain the approval of:
- (a) the Unit's Administrative Authority, and
 - (b) the University Secretary, upon recommendation of the Directory of Records sub-committee.
- 14.00 An Imaging Program must:
- (a) become established as part of a Unit's usual and ordinary course of business; and
 - (b) have established and fully-documented software systems, procedures and manuals prior to its implementation.

Plan Imaging Program

- 15.00 A proposal to initiate an Imaging Program will address the following considerations:
- 15.01 How use of this technology will be cost-effective and also ensure the Reliability and Accuracy of information and Records and their preservation for as long as required by an approved Directory of Records series retention rule.

Due to preservation concerns about electronic formats, not all Records may be suitable for imaging. Consult the University Archives for recommendations on the appropriateness of a given Imaging Program.

- 15.02 How necessary resources including but not limited to staff, Systems, and space will be assessed and provided.
- 15.03 That the storage of images shall use standard software and systems supported by University Systems. If standard software and systems cannot meet requirements, requirements must be documented and any alternative software and systems used must be compliant with University Systems requirements for security and support. Images, indices and other data about the Images should be kept in secure electronic storage; as well, backups of the Images and indices should be kept in secure off-site storage in case of disaster.
- 15.04 Identification of any legislation, regulations and university policies relevant to administration of the Records to be Imaged.
- 15.05 A description of how the Imaging Program will form part of the office's usual and ordinary course of business.

Establish Imaging Program

- 16.00 The establishment of Imaging Programs may require revisions to applicable Directory of Records series descriptions.
 - 16.01 Consultation with the University Archives on the Imaging Program will include determination of whether series revision will be necessary.
- 17.00 The procedures manual for an Imaging Program must be written prior to the implementation of the Program and accompany the proposal document as part of the approval package.
- 18.00 The procedures manual must cover the following points relating to Source Records and resulting Images.
 - 18.01 A comprehensive listing of Records series or Records types within series that are to be imaged.
 - 18.02 Steps outlined for Image capture (including steps to ensure all Records were captured).
 - 18.03 Steps outlined for indexing, to ensure Accuracy and completeness, and steps to ensure indexing is done within a reasonable time frame.
 - 18.04 The index to the Images will use the functional and series classification of the existing Directory of Records as a framework.

- 18.05 Consideration of whether optical character recognition is required, for access and reference purposes to the Images.
- 18.06 Images are checked for quality, both for readability and as an acceptable copy.
- 18.07 Ensure disposal of Source Records does not occur before Image is captured, indexed, and checked for quality.
- 18.08 Dispose of Source Records in a reasonable and regular time frame after imaging.
- 19.00 The procedures manual must cover the following points relating to the persons conducting the Imaging Program.
 - 19.01 Delegation of responsibility for imaging to person(s) conducting imaging.
 - 19.02 Person(s) who have permission to scan, edit and delete Images are defined.
 - 19.03 Person(s) who have permission to view but not edit Images are defined.
 - 19.04 Person(s) who have permission to initiate disposition of Source Records are defined.
- 20.00 The procedures manual must cover the following points relating to the security and confidentiality of Images.
 - 20.01 Steps to ensure that no Images are created, accessed, changed or deleted except by those with permission.
 - 20.02 Steps to ensure Images and index data containing personal information are kept secure and confidential in accordance with the Protection of Privacy Policy (GV0235) and Information Security Policy (IM7800). Consult the Information Security Classification Procedures for reasonable security arrangements.
 - 20.03 Steps are in place for backup and recovery of Images, indices and other data.
- Maintain Imaging Program**
- 21.00 A log of daily imaging activity is a mandatory part of the Imaging Program. If the imaging software does not automatically log the date, terminal and operator information for imaging, this must be recorded separately.

In such cases, keep a log book that shows:

- description of each Record imaged
- identity of imager and person authorizing
- date Imaged
- date Source Record destroyed
- date Image will be disposed of.

22.00 Procedures manuals and logbooks must be retained at least as long as the Images to which they pertain to ensure admissibility of Images in court once the Source Records are disposed of.

23.00 The procedures manual must always be kept up-to-date to reflect any changes in procedure and should be reviewed every 2 years. Changes in the Imaging Program must be authorized the Administrative Authority, and the University Archivist. If the University Archivist determines the proposed changes are significant enough, the Directory of Records sub-committee and the University Secretary must also approve.

Perform Disposition of Source Records

24.00 The disposition of the Source records, as described in the procedures manual, must comply with the Guidelines for the Secure Destruction and Deletion of University Records and Information.

Perform Disposition of Images

25.00 Images must be disposed of in accordance with Retention Rules in the Directory of Records, and follow the Guidelines for the Secure Destruction and Deletion of University Records and Information. Contact the Archives to carry out dispositions.

RELEVANT LEGISLATION

- [*Evidence Act \(B.C.\)*](#)
- [*Electronic Transactions Act \(B.C.\)*](#)
- [*Freedom of Information and Protection of Privacy Act \(B.C.\)*](#)
- Federal and/or provincial legislation applicable to a functional area, such as the [*Employment Standards Act \(B.C.\)*](#) or the Canada [*Income Tax Act*](#).

RELATED POLICIES AND DOCUMENTS

- Canadian General Standards Board, CAN/CGSB-72.11-93 – *Microfilm and Electronic Images as Documentary Evidence*
- Canadian General Standards Board, CAN/CGSB-72.34-2005 - *Electronic Records as Documentary Evidence*
- [*Protection of Privacy Policy \(GV0235\)*](#)
- [*Information Security Policy \(IM7800\)*](#)

RELEVANT CASE LAW

[*R. v. Oler, 2014 ABPC 130*](#)

Brief Guide to the Imaging Procedures

It is currently common to want to scan paper records taking up space in offices and storage, keep the scans, and destroy the original paper. This can improve efficiency in office workflows by making sharing easier and reducing duplication.

But hold on! There are a number of implications and risks to this. Therefore we have developed the **Procedures for the Imaging of University Records** and a risk-based assessment to determine when the procedures should be followed.

Risks and Implications

- If the records have a long retention period (e.g. longer than 7 years) or are kept permanently, the imaging must be done to high standards through a fully-documented process.
- If the scope of the imaging projects is large, e.g. an entire records classification, the imaging must be done to high standards through a fully-documented process.
- If the records are evidence of accountabilities the university has to students, staff, and faculty members, the records must be scanned accurately and reliably.

Scope of the procedures – when do they apply?

- When the project is large in scope and affects many individuals (e.g., all employee Benefits files).
- When the records are to be kept permanently by the university (e.g. Faculty members' Performance files).

Scope of the procedures – when do they likely not apply?

- When the original hard copy records are kept.
- When, for example, there is only one incoming or outgoing form.
- When there are new digital business processes where the scope of the records is limited.

Sample Proposal and Instruction documentation is available from the Archives.

The next page has a set of questions that units have to answer when contemplating any imaging, to enable assessment the proposed program and any associated risks.

Imaging Gateway Questions

Query	Why do we want to know?
1. What records are being imaged?	<i>Identification of the records</i>
2. Do the records contain confidential information, i.e. personal information or confidential business information?	<i>Confidential or Highly Confidential records require higher degrees of attention to security</i>
3. What is the DOR classification for these records?	<i>Identification of the records</i>
4. What is the retention period?	<i>Value of the records</i>
5. Is yours the primary office?	<i>Value of the records</i>
6. What format are you scanning them to?	<i>Integrity of the images – .tif and .pdf are the preferred formats</i>
7. What quality control will you perform on the scanned images (checking scanning quality)?	<i>Integrity of the records</i>
8. Where are you saving them to?	<i>Security of the records</i>
9. Who has access to these areas	<i>Security of the records</i>
10. Who administers access to these areas	<i>Security of the records</i>
11. Are you storing the images in more than one place – i.e. is there an intermediary storage location? What are the access restrictions for each of these locations?	<i>Security of the records</i>
12. What will the naming convention be for the images?	<i>Process control</i>
13. How long do you intend to keep the images in each location?	<i>Security of the records</i>
14. How long do you intend these scans to stay where you're saving them?	<i>Security and value of the records</i>
15. What are you doing with the original paper?	<i>Process control</i>
16. How soon after quality control check (7 above) do you intend to destroy the originals?	<i>Process control</i>
17. Do you have instructions for unit staff on when to dispose of the images?	<i>Process control</i>
18. Is any of the process above documented?	<i>Process control</i>
19. For existing imaging programs, how many successful retrievals occur annually (approx.)	<i>Integrity of the records</i>
20. For existing imaging programs, have any retrievals failed because the image was not clear enough or was missing?	<i>Integrity of the records</i>