The Secure Destruction of Records

Finance and Treasury Board
Provincial Archives of New Brunswick
Corporate Information Management

Table of Contents

Table of Contents

Introduction 5
Scope 5
Legal Requirements 5
Impact of the Right to Information and Protection of Privacy Act and Legal Actions 5
Principles of Records Destruction 6
1. Authorized 6
2. Appropriate 6
3. Secure/Confidential 7
4. Timely 7
5. Documented 7
Destroying Sensitive Information 8
Storage 8
Transport 8
Media and Methods of Destruction 9
1. Paper Records 9
2. Electronic/Magnetic media 9
3. CDs and DVDs 9
4. Hard Drives, Zip Disks, and Diskettes 9
5. Non-Electronic and Non-Paper Media 10
Choosing a Contract Service 10
1. Method of Destruction 10
2. Method of Transporting/Sending Records for Destruction 11
3. Certificate of Destruction 11
APPENDIX A 12
APPENDIX B 13
APPENDIX C 14

Revision History

Version	Revision Date	Author	Summary of Changes
1	*Last Review: February 2020*	CIM unit	Review of procedures
2	*Last Updated: November 2021*	CIM unit	Updated policy AD-1508 to AD-7114

Preface

The records of government are a valuable resource and an important asset that document its business activities. Their effective management enables government to support future action and decision making, reduce costs, meet business, legal and accountability requirements, and preserve New Brunswick's documentary heritage.

The Provincial Archives' Recorded Information Management Unit is responsible for the government-wide records management program under the *Archives Act*. Provincial government organizations manage their records according to corporate standards, guidelines and policies to support the delivery of their programs and services.

The Provincial Archives of New Brunswick Recorded Information Management Unit provides central records management services and support to departments, crown corporations and agencies within the government of New Brunswick by:

- developing and authorizing retention and disposition schedules that control the period of time government records are retained as well as their final disposition through the transfer to the Provincial Archives or destruction;
- developing and establishing policy, standards and guidelines;
- providing training, technical and consultative services in the development, implementation and maintenance of programs to manage recorded information in all formats;
- identifying archival and records management issues at the beginning of the information life cycle.

Departments manage recorded information by:

- applying the *Classification Plan and Retention Schedules for Common Records* for retention scheduling;
- establishing a file classification plan for operational records;
- developing and maintaining written policies and procedures;
- cooperating with the Provincial Archives to develop and apply retention and disposition schedules for all government records in all formats*;*
- taking advantage of the centralized records storage and retrieval services of the Provincial Archives Records Centre.

It is important to note that records must not be destroyed or removed from the control of the Government of New Brunswick, unless such action is authorized under the *Archives Act*.

Introduction

Recorded information of the Government of New Brunswick, regardless of format, must be maintained and disposed of in a secure manner. The following guidelines are intended to assist government bodies in determining the appropriate method for the secure destruction of records.

Scope

These guidelines apply to all public bodies as defined in the *Archives Act*.

These guidelines can be used and applied to both public records and non-records containing information of a personal or sensitive nature. Although non-records do not meet the criteria of a public record, proper care should be taken with their disposal. For more information on identifying what is or is not considered a public record and how to manage them, see the *Guide to Identifying and Handling Non-records.*

Legal Requirements

Nothing within these guidelines is to be interpreted as authorization to destroy a public record that belongs to the Province of New Brunswick. Public records can only be disposed of in accordance with an authorized Records Retention and Disposition Schedule, approved by the Provincial Archivist, and as described in the Archives Act.

According to the *Information Management Policy AD-7114* departments are responsible for the security of records in their custody.

Impact of the Right to Information and Protection of Privacy Act and Legal Actions

In situations involving an access request or legal action, caution is required.

At the time an access request is received, all existing relevant information is part of that request. As such, information (whether it is a public record or a non-record) cannot be destroyed until the request is processed and any appeal period has expired.

Due concern and diligence must also be taken concerning recorded information relating to ongoing legal action, such as discovery processes and legal holds. In such cases, recorded information cannot be disposed of until the hold is lifted.

Principles of Records Destruction

1. Authorized

Authorization by Provincial Archives

The destruction of records must be authorized by an approved retention and disposition schedule established by the Provincial Archivist in accordance with the *Archives Act.*

Authorization by the Department

The Provincial Archivist establishes a Records Retention and Disposition Schedule in accordance with the *Archives Act*. A Records Retention and Disposition Schedule is a legal document that provides a description of a records series (group of records) and explains the purpose of the series. It specifies the length of time the records are active in the office, and how long they must be stored before final disposition - whether they are stored at the Provincial Archives' Records Centre or another off-site location. Disposition includes the transfer of a body of records to the Provincial Archives for permanent retention or archival selection, or destruction. Although records retention and disposition schedules are authorized by the Provincial Archivist, they are agreed to jointly by the records-creating department or agency.

When records in semi-active storage at the Records Centre are due for destruction according to a Records Retention and Disposition Schedule, the Records Manager of the department or public body responsible for those records is sent a Disposition Notice Form. The records manager reviews the records to ensure that they are not required for pending legal actions, a Right to Information request, or for any other reason. Once the determination has been made to proceed with destruction, the Records Manager or an appointed designate authorizes the destruction of the records by signing the Disposition Notice Form and returning it to Records Centre Staff.

Where a records retention and disposition schedule establishes that records are not sent to the Records Centre for semi-active storage the responsibility for carrying out the secure destruction lies with the department or public body. A staff member of the department or public body, generally the Records Manager, must ensure that the records remain protected against unauthorized access up to and during the act of destruction, and that the method of destruction is appropriate and permanent to prevent reassembly or recovery.

For the destruction of records in-house, or non-records containing personal or sensitive information such as a note pad with an individual's name, address, telephone number, or social insurance number, it is recommended that a *Records Destruction Form* **(**Appendix A**)** be used in order to document, track, and authorize the action.

2. Appropriate

Appropriate methods for destroying records must be implemented to ensure the destruction process is irreversible, environmentally friendly, and meets the necessary security requirements (see also 1.3 & 4.0).

Irreversible

Irreversible destruction of records means that there is no reasonable risk of the information being recovered or reconstituted. Failure to ensure the complete destruction of records may lead to the unauthorized release of information and a violation of the *Right to Information and Protection of Privacy Act (RTIPPA)*, the *Archives Act*, and/or other legislation which mandates or regulates the disclosure of specific types or categories of information.

Environmentally Friendly

Records should be destroyed in a manner as environmentally friendly as possible. Both paper and microfilm should be recycled, wherever possible.

3. Secure/Confidential

The level of security applied during the active and semi-active periods of the records must continue to apply through to the completion of their destruction. When highly sensitive, confidential, or personal/identifiable information is being destroyed, the process should be supervised by an authorized representative of the department or should be well documented if contracting through a third party.

4. Timely

While it is important not to destroy records before the authorized disposition date, it is equally important not to keep records longer than necessary. Once records are no longer required to meet legal or administrative needs, they should be promptly destroyed according to an approved records retention and disposition schedule.

If a legal action or right to information request requires the maintenance of records past their scheduled retention and disposition period, documentation of the authorization for the hold and reason for the decision should be kept as a record.

5. Documented

It is important that the process of destroying records is well documented as evidence of the destruction may be vital in cases of legal proceedings or right to information requests.

The information documenting the destruction should include:

- the records series title and number of the approved records retention and disposition schedule
- disposition date
- signature of the designated person authorizing the destruction
- the name of the person or service provider responsible for the destruction
- confirmation from the person or contractor that the records have been destroyed (Certificate of Destruction).

For sample contract clauses for the destruction of records see Appendix C.

Destroying Sensitive Information

Particular care and attention must be paid to the handling of records containing sensitive information. The level of security applied during the lifecycle of these records should be maintained up to and during the destruction process.

GNB information is classified based upon the following levels and definitions:

Levels	A breach of the security of information classified at this level . . .
High	Could reasonably be expected to cause extremely serious personal or enterprise injury, including any combination of a) extremely significant financial loss, b) loss of life or public safety, c) loss of confidence in the government, d) social hardship, or e) major political or economic impact
Medium	Could reasonably be expected to cause serious personal or enterprise injury, including any combination of a) loss of competitive advantage, b) loss of confidence in the government program, c) significant financial loss, d) legal action, or e) damage to partnerships, relationships and reputations.
Low	Could reasonably be expected to cause significant injury to individuals or enterprises including any combination of a) limited financial losses, b) limited impact in service level, or c) performance, embarrassment and inconvenience
Unclassified	Will not result in injury to individuals, governments or to private sector institutions and financial loss would be insignificant. This would be considered a public document.

(*Government Information Technology Systems Security Policy*)

Storage

Records waiting for destruction or disposition should remain inaccessible to unauthorized personnel at all times to safeguard them from loss, unauthorized destruction, or alteration. Departments and public bodies are responsible for the development and implementation of procedures concerning the secure storage of records. Storage containers with restricted access should be monitored and properly maintained. Changes in access rights should be recorded as required.

Transport

Maintaining restricted access to records being transmitted from an individual or place to another is of utmost importance. Records should be packaged appropriately and should be unidentifiable where necessary. Only reliable postal or courier services should be used. Vehicles used for transport should be closed and secure, and containers should also be closed during transport.

Media and Methods of Destruction

1. Paper Records

Depending on the sensitivity level of records, paper and other hardcopy records may be recycled, shredded, mangled, mulched, or otherwise processed ensuring that the recorded information has been obliterated and made irrecoverable.

Recycling

Paper records considered to be of low sensitivity may be destroyed by recycling in office where they are then sent to the Solid Waste Commission.

Shredding

If shredding is the preferred method, consideration should be given to how the paper is shredded. Sensitive material may require cross shredding or more than one shredding cycle. Paper records considered to be high risk or of a sensitive nature should be shredded as soon as they have reached their disposition date. This may be done in office, on site by a third-party contractor, or sent to the Solid Waste Commission for shredding, and a certificate of destruction should be obtained. Public bodies should ensure that authorized personnel are present to monitor the destruction of highly sensitive information.

2. Electronic/Magnetic media

Electronic or magnetic media includes CDs and DVDs, hard disk drives, and zip drives or diskettes.
Information in electronic form is considered “destroyed” in accordance with the terms of a records schedule when:

- the information is rendered unreadable and irretrievable by either being securely erased or overwritten by system software, or
- the disk, hard-drive or other electronic object or device upon which the information was stored has been destroyed or physically damaged so that it is no longer possible to recover the information.

3. CDs and DVDs

All CDs and DVDs should be treated as a single use storage medium as they have no secure erase capability. As a result, once the information contained on CDs and DVDs has reached its date of disposition, the disks must be physically destroyed. If the information they contain is of a personal or sensitive nature, then the disks must be shredded, either in-house of through a third party. A record confirming their destruction must be kept (see section 1.5).

4. Hard Drives, Zip Disks, and Diskettes

It is important to note that the delete/erase function of most operating systems does not result in the secure destruction of the information they contain. This includes hard drives

found in photocopiers, printers, and fax machines. As a rule, all public records should be stored to a network hard drive where the data is backed up according to a regular schedule.

If a hard drive, zip drive, or diskette is to be transferred to a new owner within the same department once the date of disposition has been reached, it should be reformatted so that special recovery tools necessary to access the records would be required. If the hard drive, zip drive, or diskette contains records of a personal or sensitive nature, they must be securely erased or sanitized (for more information on the full list of procedures required, contact the Chief Information Office).

Note: In many cases, it is more economical to physically destroy zip disks and diskettes rather than have them securely erased.

If a hard drive, zip drive, or diskette is to be transferred outside its original department or outside the custody of the Province once its disposition date has been reached, all recorded information is to be securely erased using disk wiping procedures as set out by the Chief Information Office. A record guaranteeing the information has been properly wiped must be maintained (see Principle 5).

Any hard drive, zip drive, or diskette which has reached its disposition date, and which is inoperable or damaged should be physically destroyed or shredded.

5. Non-Electronic and Non-Paper Media

Other types of recorded information mediums including video tape, film and microform (aperture cards, fiche, microfilm, x-rays) can be successfully destroyed by shredding, cutting, crushing or chemical recycling. It is important to note that silver halide microfilm cannot be disposed of like regular waste as it is considered hazardous material. Although the solid waste commissions in New Brunswick do not currently accept silver halide microfilm, there are several companies that provide a silver recovery/recycling service such as Terrapure Environmental, based in New Brunswick and Clean Harbors, based in Nova Scotia.

Choosing a Contract Service

When contracting out the destruction of records, it is the department's responsibility to ensure that the appropriate methods of destruction are used. There are several factors involved in choosing the right contractor including:

1. Method of Destruction

The contractor must be able to provide the appropriate method of shredding. This may include recycling, multiple shredding cycles for sensitive records, or the capability to shred electronic or metallic devices.

2. Method of Transporting/Sending Records for Destruction

Records may be picked up by the contractor or delivered by the department. In either case, the vehicle used for transport should be closed and secure. If an open truck is used, ensure that the containers are covered securely. When transporting records of a sensitive nature, only a vehicle that is closed and lockable should be used. Records waiting for pick up or in transit must continue to be secured against loss, theft, and unauthorized access.

It is advisable to include in the contract a provision whereby the records are guaranteed to be kept secure and inaccessible at all times while in transit or on site.

3. Certificate of Destruction

A contractual agreement with a service provider should include a certificate of destruction that includes the method used. If a case arises where records contracted to be destroyed are later found or recovered, this certificate is evidence that the contractor is at fault.

For sample contract clauses for the secure destruction of records, see Appendix C.

For your convenience, a Records Destruction Checklist is provided, see Appendix B.

APPENDIX A

RECORDS DESTRUCTION CHECKLIST

____ 1. Records are authorized for destruction according to an approved Records Retention and Disposition Schedule (Final Disposition is D).

____ 2. Records have reached the end of their lifecycle.

____ 3. Records are not subject to:

□ a Right to Information request
□ an ongoing legal action
□ a legal hold
□ an e-discovery request

____ 4. Departmental authorization for destruction has been obtained.

____ 5. Appropriate service provider has been contacted.

____ 6. Approved methods of destruction have been specified

□ Recycling
□ Shredding
□ Cross Shredding
□ Pulverization/incineration

____ 7. Destruction of sensitive information was supervised by an authorized representative of the department.

____ 8. Confirmation that the records were destroyed has been received.

____ 9. Details of the destruction have been recorded.

APPENDIX B

RECORDS DESTRUCTION FORM / FORMULAIRE POUR LA DESTRUCTION DES DOCUMENTS

DEPARTMENT / MINISTÈRE:

BRANCH/DIRECTION	RECORDS DESCRIPTION/DESCRIPTION DES DOCUMENTS	DATES OF RECORDS/ DATES DES DOCUMENTS	SCHEDULE NUMBER/ NUMÉRO DE CALENDRIER	DATE DESTROYED/ DATE DE DESTRUCTION	APPROVED BY/ APPROUVÉ PAR

APPENDIX C

SAMPLE CONTRACT CLAUSES FOR THE SECURE DESTRUCTION OF RECORDS

- [Company] agrees to maintain security standards consistent with security policies of the Government of New Brunswick. These include strict control of access to data and maintaining confidentiality of information gained while carrying out its duty.
- [Company] must assure that all employees handling high risk or sensitive information have passed a criminal record check and that the results are negative.
- Material, data, and information accessed or developed in the course of the delivery of the work described in the contract is confidential and the property of the Province of New Brunswick.
- [Company] agrees that under no circumstances are materials sent for destruction to be used for purposes other than meeting the terms and conditions of the contract.
- [Company] agrees that it will destroy records collected from [Client] in the following manner:
    - [Specify manner of destruction. Records should be destroyed using a method appropriate to their security level.]
- [Company] agrees that its services will be performed in a professional manner, in accordance with industry standards and practices by properly trained employees. [Company's] employees understand that a breach of the security and confidentiality of [Client's] information may lead to disciplinary measures.
- If [Company] engages the services of a third party to perform all or part of the services under this contract, [Company] takes overall responsibility for the successful delivery of the work described in the contract. A copy of the subcontract between [Company] and a third party shall be provided to [Client] at the time it is entered into.
- If [Company] engages the services of a third party to perform all or part of the services under this contract, the third party shall agree, in a written contact with [Company] to comply with all standards and procedures required of [Company] by [Client]. [Client's] records will not be transferred to a third party other than for the purposes of performing destruction under such a subcontract.
- [Company] shall provide [Client] with a Certificate of Destruction documenting the date, time, location, and method of destruction and bearing the signature of the operator, either at the conclusion of the destruction process or, if destruction is performed as part of a regularly scheduled event, at specified regular intervals as agreed to by [Company] and [Client].

- If request by [Client], a designated staff of the Government of New Brunswick may observe and inspect destruction process, site, and activity of the [Company] at any reasonable, unscheduled time.
- [Company] agrees that any records collected from [Client] for the purpose of destruction will be destroyed within [xx] days of collection. During transport or pending their destruction, the records shall be stored in a secure manner, ensuring physical security and restricted access. [Company] will know at all times the location of [Client's] records and will advise the [Client] of this location if requested.
- [Company] must be able to provide a copy of liability and damage insurance, along with proof of good standing with the Workers Compensation Commission.

Note: The abovementioned sample contract clauses are **not** intended to provide legal advice and must **not** be construed as such