Government of Canada | Gouvernement du Canada

Canadian General Standards Board | Office des normes générales du Canada

CAN/CGSB-72.34-2024

Supersedes CAN/CGSB-72.34-2017
Reaffirmed March 2022

Electronic records as documentary evidence

Canadian General Standards Board CGSB

SCC CCN

Canada

Experience and excellence
Expérience et excellence
CGSB ONGC

Canadian General Standards Board statement

The CANADIAN GENERAL STANDARDS BOARD (CGSB), under whose auspices this standard has been developed, is a government directorate within Public Services and Procurement Canada. CGSB is engaged in the production of voluntary standards in a wide range of subject areas through the media of standards committees and the consensus process. The standards committees are composed of representatives of relevant interests including producers, consumers and other users, retailers, governments, educational institutions, technical, professional and trade societies, and research and testing organizations. Any given standard is developed on the consensus of views expressed by such representatives.

CGSB has been accredited by the Standards Council of Canada as a national Standards Development Organization. The standards that CGSB develops and offers as National Standards of Canada conform to the requirements and guidance established for this purpose by the Standards Council of Canada. In addition to standards it publishes as National Standards of Canada, CGSB may produce other deliverables that meet particular needs, in response to requests from a variety of sources in both the public and private sectors. CGSB standards and CGSB's National Standards are developed in conformance with the policies described in the CGSB Policy and Procedures Manual for the Development and Maintenance of Standards.

CGSB's standards are subject to review and revision to ensure that they keep abreast of technological progress. CGSB will review and publish this standard on a schedule not to exceed five years from the date of publication. Suggestions for their improvement, which are always welcome, should be brought to the notice of the standards committees concerned. Changes to standards may be issued as amendments or as new editions of standards.

An up-to-date listing of CGSB's standards, including details on latest issues and amendments, is found in the CGSB Catalogue at the following Web site, http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html, along with more information about CGSB products and services.

Although the intended primary application of this standard is stated in its scope, it is important to note that it remains the responsibility of the users of the standard to judge its suitability for their particular purpose.

The testing and evaluation of a product or service against this standard may require the use of materials and/or equipment that could be hazardous. This standard does not purport to address all the safety aspects associated with its use. Anyone using this standard has the responsibility to consult the appropriate authorities and to establish appropriate health and safety practices in conjunction with any applicable regulatory requirements prior to its use. CGSB neither assumes nor accepts any responsibility for any injury or damage that may occur during or as the result of tests, wherever performed.

Attention is drawn to the possibility that some of the elements of this standard may be the subject of patent rights. CGSB shall not be held responsible for identifying any or all such patent rights. Users of this standard are expressly advised that determination of the validity of any such patent rights is entirely their own responsibility.

For enforcement purposes, standards shall be considered published the final day of the month of their publication date.

Contact the Canadian General Standards Board

To obtain information on CGSB, its services and standards or to obtain CGSB publications, please contact us:

web — http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html

e-mail — ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca

telephone — 1-800-665-2472

mail — Canadian General Standards Board
140 O'Connor Street, Tower East
Ottawa, Ontario Canada K1A 0S5

Standards Council of Canada statement

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

NATIONAL STANDARD OF CANADA

CAN/CGSB-72.34-2024

Supersedes CAN/CGSB-72.34-2017
Reaffirmed March 2022

Electronic records as documentary evidence

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE.

ICS 37.080

Published June 2024 by the
Canadian General Standards Board
Ottawa, Ontario K1A 0S5

Canadian General Standards Board

Committee on Electronic Records and Image Management

(Voting membership at date of ballot)

Chair (non-voting)

Luciana Duranti	InterPARES (General interest)

General interest category

Corinne Rogers	InterPARES
Jake V. Knoppers	Consultant
Lois M. Evans	Land Title and Survey Authority of British Columbia
Louise Spiteri	Dalhousie University
Stuart Rennie	Records Management Consultant

Producer category

Daryl Stott	Nimble Information Strategies Inc.
Raj Krishnamoorthy	Deloitte LLP
Richard Davis	Data Repro Com Limited
Robert Gerbrandt	Iron Mountain
Tracy Caughell	Open Text Corporation

Regulator category

David Charles	Canada Revenue Agency
Maryse Kiese	Canada Border Services Agency
Michael Mohammed	Treasury Board of Canada Secretariat

User category

Heather Houston	Public Services and Procurement Canada
Rebecka Sheffield	Association of Canadian Archivists
Robert Weisman	University of Ottawa
Sharon Smith	Library and Archives Canada
Uta Fox	Calgary Police Service

Committee Manager (non-voting)

Robert Long	Canadian General Standards Board

Acknowledgment is made to Corinne Rogers and Lois M. Evans for leading the working group in the revision of the latest edition of this standard.

Translation of this National Standard of Canada was conducted by the Government of Canada.

Preface

This National Standard of Canada CAN/CGSB-72.34-2024 supersedes the 2017 edition including its October 2018 Amendment and March 2022 reaffirmation.

Changes since the previous edition

The changes signify a minor revision, focused on correcting omissions, factual errors, redundancies within the standard, duplication within the Standard of recognized best practices available in other standards or knowledge bases and clarity. Noteworthy changes are:

- Updates to Section 3 Terms and definitions. Unused terms removed, several terms clarified, new terms added.
- Updates to Section 5 Legal requirements. Edited for clarity.
- Updates to Section 6 Records management program. Major and minor changes made to enhance clarity and improve focus on essential information.
- Updates to Section 7 IT system management. Made this a standalone section, strengthened sections on risk assessment and privacy, introduced 7.4 Security and protection.
- Informative appendices deleted and essential information moved to body of standard.
- Bibliography. Reviewed and updated all citations.

The following definitions apply in understanding how to implement this National Standard of Canada:

- "shall" indicates a **requirement**;
- "should" indicates a **recommendation**;
- "may" is used to indicate that something is **permitted**;
- "can" is used to indicate that something is **possible**, for example, that an organization is able to do something.

Notes accompanying clauses do not include requirements or alternative requirements. The purpose of a note accompanying a clause is to separate explanatory or informative material from the text. Annexes are designated normative (mandatory) or informative (non-mandatory) to define their application.

Table of contents

Page

Foreword

CAN/CGSB-72.34 specifies principles, methods, and practices for the creation (i.e. making, receipt, and capture) and management of all forms of electronic records (e.g. e-mail, cartographic, audio-visual, textual, multimedia, etc.) to support their admissibility [see admissibility (records), admissibility (rules), and weight (of evidence)] as evidences in legal proceedings. Because this standard provides only general legal, management and technical information, users should seek further advice before applying its recommendations to specific records or systems.

This standard is harmonized with applicable federal, provincial and territorial acts in force and their pursuant regulation at the time of the Committee's deliberations. Where differences exist between an act or a regulation and this standard, the former will prevail.

Introduction

About this standard

An organization may be required to produce electronic records as evidence in legal proceedings. To support the admissibility and weight of electronic records as documentary evidence, the organization needs to ensure that these records can be proven or presumed to be reliable, accurate, and authentic, that is, trustworthy. To ensure the trustworthiness of their electronic records, an organization should comply with this standard.

This standard uses the term “electronic record” rather than “digital record.” Whereas the term “digital record” refers to a record composed of discrete binary values aggregated into one or more bit streams, the term “electronic record” encompasses any digital record, as well as any analogue record that is carried by an electrical conductor and requires the use of electronic equipment to be made readable by an individual.

This standard is information technology neutral, in that it neither assumes nor endorses any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation. This standard supports an integrated, interoperable electronic records management system approach.

This standard provides a framework and guidelines for the implementation and operation of records systems for electronic records, whether or not any information held therein will ever be required as evidence. Thus, compliance with it should be regarded as a demonstration of responsible business management. Applying the standard to an organization’s business will not eliminate the possibility of litigation, but the probability is that it will make the production of electronic records easier and their acceptance in a legal procedure more certain.

Relationship to Canadian legal evidentiary requirements

Records recorded by or stored in an electronic technology may be admissible as evidence in Canadian legal proceedings. If their admissibility is challenged, the records will need to satisfy certain statutory and, in some cases, common law admissibility requirements. These requirements may vary depending on the purpose for which the records are offered into evidence. The *Canada Evidence Act*, as well as most provincial and territorial Evidence Acts, contains the following provision, encouraging the use of standards:

“For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.”

Use of this standard in legal proceedings

In legal proceedings, this standard could inform the development of arguments about the definitions of the key phrases of the rules of admissibility for electronic records. These phrases are “IT system integrity” and “record integrity,” as used in the electronic record provisions of the Evidence Acts, and records “made in the usual and ordinary course of business” as used in the CEA.

Terms and definitions

This standard uses terms and definitions derived from relevant national and international standards, guidelines, and policies.

English and French versions of this standard

To ensure agreement between the English and French versions, the following principles have been adhered to. Where the English version utilizes “record,” the French equivalent “enregistrement” is used in the French version. Whenever the English version utilizes “document,” the French equivalent “document” is used in the French version.

The French version of CAN/CGSB-72.34 differs from the international French for some terms, because of Canadian usage. For example, the terms “final disposition,” “preservation,” “record,” and “records management” in the English version are translated as “élimination,” “préservation,” “enregistrement,” and “gestion des enregistrements” respectively.

Electronic records as documentary evidence

1 Scope

1.1 This National Standard of Canada provides guidance for developing policies, procedures, processes and documentation that support the continuing reliability, accuracy and authenticity of electronic records to:

a) ensure that electronic records can reliably support business decisions and exchanges of commitments;

b) support the admissibility and the weight of electronic records in legal proceedings; and

c) protect the capability of electronic records to effectively document an organization's decisions, actions, and transactions and to hold accountable those who are responsible for them.

1.2 This standard applies to organizations that make, receive, capture, maintain, manage, use, transmit, dispose or store recorded information electronically, and to private and public sector activities, irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

1.3 This standard is intended to ensure that electronic records in records systems are trustworthy. Typical users include:

a) managers of private and public sector organizations;

b) IT systems and records management professionals;

c) legal professionals and those responsible for security services and risk management; and

d) other individuals responsible for creating (i.e. making or receiving, or storing) and maintaining an organization's records.

1.4 This standard outlines methods for the management and preservation of electronic recorded information that are regarded as best practices independently of legal considerations. Therefore, organizations conforming to this standard benefit even when evidentiary issues are not in question.

1.5 In addition, this standard provides guidelines for a procedural framework supporting quality practices in records management; and identifying and implementing appropriate measures to protect the evidentiary value of electronic records, including their incorporation within records and IT systems design and management processes.

2 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this National Standard of Canada. The referenced documents may be obtained from the source noted below.

Note: The contact information provided below was valid at the date of publication of this standard.

An undated reference is to the latest edition or revision of the reference or document in question, unless otherwise specified by the authority applying this standard. A dated reference is to the specified revision or edition of the reference or document in question.

2.1 Department of Justice

Canada Evidence Act (CEA)

Personal Information Protection and Electronic Documents Act (PIPEDA)

2.1.1 Contact information

The above may be obtained from the Department of Justice Canada, Communications Branch, Public Affairs Division. Telephone: 613-957-4222. Web site: http://canada.justice.gc.ca.

2.2 Evidence Acts of each provincial and territorial jurisdiction may be obtained from their respective Justice Laws Web sites.

2.3 Other sources considered in the development of this standard are listed in Annex A.

3 Terms and definitions

For the purposes of this National Standard of Canada, the following terms and definitions apply.

access
right, opportunity, or means of finding, consulting or retrieving recorded information.

access control
process of allowing only authorized individuals to have access to records in the records system.

accountability
principle that individuals and organizations, being responsible for their actions, may be required to provide an account of them.

accuracy
degree to which recorded information is precise, correct, truthful, free of error or distortion.

admissibility (records)
capability of recorded information to be introduced as evidence in a legal proceeding.

admissibility (rules)
rules by which records are judged to be acceptable as evidence in legal proceedings.

analogue record
record written as a continuous signal on physical material, such as a paper, film, audio and videotape.
See also *record*.

artificial intelligence
information technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours, or solving problems.

audit
systematic review of recorded information activities for compliance with policies, procedures, and controls are established and complied with to meet all financial, operational, legal, and regulatory obligations.

audit trail
log of IT system activities that enables the reconstruction, reviewing and examination of the sequence of activities relating to an operation, a procedure, or an event in a transaction.

authentic record
record that is what it purports to be and that is free from tampering or corruption.

authentication
declaration of authenticity at a given point in time.

authenticity
quality of an entity that it is what it purports to be and that it is free from tampering or corruption.

authorized individual
individual who is given a specific responsibility by an authority who has the power to do so.

automated decision system
includes any technology that either assists or replaces the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural networks.

backup (copy)
an exact copy of active electronic systems, programs, information and data made for the purpose of recovery in the event of a system malfunction.

capture
act of recording or saving a particular instance of recorded information.

cloud computing
model for enabling ubiquitous and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

conversion
process of changing recorded information from one format to another.
See also *migration*.

copy
duplicated recorded information.

data
smallest meaningful unit of recorded information.

destruction (records)
process of eliminating records beyond any possibility of reconstruction.

digital record
record composed of discrete binary values aggregated into one or more bit streams accessed by a computer.

digitization
process of converting analogue recorded information to digital form.
See also *analogue record*.

disposition (records)
final action taken on a record that has met its prescribed retention period.

document
indivisible unit of recorded information having stable content and fixed form.

documentary evidence
recorded information admitted as evidence in legal proceedings.

electronic discovery (e-discovery)
pre-trial procedure requiring an exchange of relevant recorded information among the parties.

electronic record
analogue or digital record accessed using electronic equipment.
See also *record* and *analogue record*.

encryption
conversion of recorded information into a secret code (or plain text into cipher text).

evidence
all means by which any alleged matter of fact, the truth of which is submitted to investigation, is established or disproved in a legal proceeding.

format
means of encoding data to contain information about its structure, organization, and content so that it can be interpreted for future use in storage, retrieval, processing, presentation, manipulation, and transmission activities.

hearsay
out-of-court statement by someone other than the individual who is testifying and which is submitted for the truth of the facts in the statement.

information
message intended for communication.

information security
multidimensional discipline designed to keep recorded information in all locations free from any threat by a combination of mechanisms (technical, organizational, human-oriented, and legal).

IT system
set of one or more computers, associated software, peripherals, terminals, human operations, physical processes, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer.

IT system integrity
proven capability of an IT system to perform its intended functions in an unimpaired manner, free from unauthorized manipulation, whether intentional or accidental, and the fact that it did so when the recorded information was generated and used.

IT system malfunction
technical problem, defect, failure, or disaster in the functioning of an IT system.

IT system reliability
quality of a system that has been tested, subjected to peer review or publication, accepted within the relevant scientific community and whose known or potential error rate is acceptable.

legal hold
process whereby an organization preserves all forms of potentially relevant records when litigation is reasonably anticipated or underway.

medium
physical storage material to which recorded information is affixed.

metadata
attributes that identify a record and describe its use, management, custodial history, and technological changes.

migration
process of moving recorded information from one IT system configuration to another.
See also *conversion*.

official record
instance of a record that has the force of an original record and is authoritative, final, and complete.

organization
entity capable of having legal rights and duties.

original record
first complete record capable of reaching the purposes for which it was intended (i.e. effective).

Note: An original record has three characteristics: primitiveness (i.e., the first to be generated); completeness; and effectiveness.

preservation (records)
whole of the principles, policies, and strategies that controls the activities designed to ensure the records' physical and technological stabilization and protection of intellectual content through time.

probative value
weight or credibility given to evidence.
See also *weight*.

procedure
rules governing the conduct of a transaction, or the formal steps undertaken in carrying out a transaction.

process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result.

quality assurance (records)
procedures for monitoring and assessing the records system, aiming to maintain a desired level of quality.

record
any document made or received by an organization in the course and by reason of its activity, and kept for further action or reference.

record identity
whole of the attributes of a record that together uniquely identify it and distinguish it from any other record.

Note: With record integrity, a component of authenticity.

record integrity
quality of being complete and unaltered in all essential respects.

Note: With record identity, a component of authenticity.

recorded information
information affixed to a medium in a stable form.

recordkeeping
capture, storage, use, maintenance and disposition of records and their metadata.

records classification
systematic organization of records in groups or categories according to methods, procedures, or conventions represented in a plan or scheme.

records lifecycle
model of records management and archival science that characterizes the life span of a record in sequential stages: creation (making, receiving or capturing); classification; maintenance and use; appraisal; disposition through destruction or transfer to an archival institution or agency; preservation; description in archival finding aids; and reference and access.

records management
field of management concerned with the creation (making, receiving or capturing), maintenance, use and disposition of records.

records management manual
document that defines the scope of the records management program, its authority, the services it provides, and the fundamental records management concepts.

records management program
program designed to support the creation, management, use, disposition and preservation of trustworthy records.

records retention period
specified period of time that records are kept to meet operational, legal, regulatory, fiscal or other requirements.

records system
a computer system by or in which information is recorded or stored and any related procedures.

reliability
quality of a record, the content of which can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests.

risk assessment
evaluation of the probability of an adverse event and of the extent of its impact to prepare for it.

secure electronic signature
electronic signature that results from the application of a technology or process prescribed by the Secure Electronic Signature Regulations (SOR/2005-30) made under subsection 48(1) of the PIPEDA.

source record (digitization)
analogue record from which a digital copy is made.
See also *analogue record*.

spoliation
act of destroying, altering or concealing evidence.

transitory record
record to which no retention requirement applies, and which has no enduring value in documenting or supporting the organization’s business.

trustworthy record
record that is accurate, reliable and authentic.
See also *accuracy*, *reliability* and *authenticity*.

weight (of evidence)
credibility or probative value of evidence.

4 Acronyms and abbreviated terms

The following acronyms and abbreviations are used in this standard:

CEA	*Canada Evidence Act*
IT	Information Technology
PIPEDA	*Personal Information Protection and Electronic Documents Act*
RM	Records Management
RO	Records Officer
S.	Section
Subs.	Subsection
TAR	Technology-Assisted Review

5 Legal requirements for electronic records as documentary evidence

5.1 General

The primary principle advanced by this standard is that an organization shall always be prepared to produce its records as evidence. The organization shall maintain control of its recorded information at all times including where remote work is in place.

Continuous compliance with this standard is an essential part of the proof of the integrity of an electronic record or records system. Intermittent compliance may be better than no compliance, but it is not enough to prove the integrity. Therefore, compliance obtained only when legal proceedings are anticipated or are underway is not sufficient.

Sections of the *Canada Evidence Act* (CEA) cited below apply only to legal proceedings governed by federal laws:

a) original paper records, admissible as business records under provisions such as s. 30 of the CEA;

b) electronic records, admissible under provisions such as s. 31 of the CEA;

c) microfilmed, digitized, or imaged records, admissible under the copy provisions such as s. 30 of the CEA, or the electronic records provisions such as s. 31 of the CEA;

d) “relied upon printouts” of electronic records, admissible under provisions such as subs. 31.2(2) of the CEA; or

e) records created through electronic data interchange (EDI), admissible under provisions such as s. 31 of the CEA.

There are comparable provisions in the laws of the provinces and territories for legal proceedings governed by the laws in those jurisdictions.

Because the laws and standards governing the admissibility as evidence of electronic and paper records differ, management of these records may also differ. The laws of evidence applying to legal proceedings in the federal and provincial/territorial jurisdictions permit electronic documents (or records), including electronic images, to stand in the place of original paper source records, or their copies. To be admissible, an electronically-produced record of any kind shall satisfy the electronic record provisions of the law in the jurisdiction involved.

5.2 Requirements for admissibility of electronic records as documentary evidence

Use of an electronic record as evidence requires proof of the authenticity of the record, which can be inferred from the integrity of the electronic records system in which the record is made or received or stored, and proof that the record was “made in the usual and ordinary course of business” or is otherwise exempt from the legal rule barring hearsay (see s. 30 of the CEA for example).

5.2.1 Authenticity of the record

A record submitted as evidence shall be authenticated by providing evidence external to the record itself (e.g., the testimony of a witness to the making of the record) that it is what it purports to be (its identity and integrity are intact), see s. 31.1 of the CEA. This is the authentication rule. Alternatively, a record can be declared authentic if the integrity of the records system in which the record was made or received, or stored, and/or the reliability of the recordkeeping processes, can be proven.

5.2.2 Integrity of the electronic records system

If a party offers a record into evidence to prove the truth of its content, the best evidence rule applies. The best evidence rule prefers the original of a record (or primary evidence) over its copies (or secondary evidence). In cases where more than one instance of a record exists, an organization shall identify which instance constitutes the organization’s official record (primary evidence).

If the party offering the secondary evidence can satisfactorily explain the absence of the primary evidence so as to refute any suggestion of fraud, then the secondary evidence is admissible. With electronic records, the application of the best evidence rule is problematic due to the absence in the digital environment of what is traditionally considered an original. Therefore the law of evidence provides that the best evidence rule can be satisfied by proof of the integrity of the records system, as in subs. 31.2(1)(a) of the CEA.

Such “integrity” is proven, in the absence of evidence to the contrary, by evidence that

a) the electronic records system was at all material times operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the system. (e.g. subs. 31.3(a) of the CEA); or

b) the electronic record was recorded or stored by a party who is adverse in interest to the party seeking to introduce it into evidence (e.g., subs. 31.3(b) of the CEA); or

c) the electronic record was recorded or stored in the “usual and ordinary course of business” by a person who is not a party to the proceedings, and who was not under the control of the party seeking to introduce it (e.g., subs. 31.3(c) of the CEA).

5.2.3 Record made in the “usual and ordinary course of business”

If a party offers a record into evidence for the proof of its contents, the hearsay rule also applies (see hearsay). An exception to the hearsay rule is made for business records on the assumption that organizations would use records procedures which ensure the reliability of the recorded information. The business records exception to the hearsay rule is satisfied by proof that the record in question was made in the “usual and ordinary course of business” of the organization from which the record comes (e.g., s. 30 of the CEA). The term “business” is given a wide definition to include, “any business, profession, trade, calling, manufacture or undertaking of any kind carried on in Canada or elsewhere whether for profit or otherwise” (e.g., subs. 30(12) of the CEA).

Just as is the case with the authentication rule and the best evidence rule, the application of the business records exception to the hearsay rule relies on proof of the integrity of the records system in which the record submitted as evidence was made or received or stored.

5.2.4 Proof of the integrity of an organization's records system

The following factors can be used to prove the integrity of an organization's electronic records system:

a) sources: the origin of the data in records in the electronic system is known;

b) contemporaneous recording: the electronic records are made or received or stored within a reasonable time after the events to which they relate, or stored within a reasonable time after they are received;

c) routine business data: the data within a record is of a type regularly supplied to the originating organization, or created by it during its regular activities;

d) data entry: the data entry procedures are part of the usual and ordinary course of business of the organization, and are carried out in compliance with the RM manual and IT system management guide (see 6.4 and 6.5);

e) standards: the organization complies with applicable electronic records management standards as per 6.3.2. b);

f) decision making: the organization, when making decisions, relies upon the electronic records in its electronic records system;

g) software: the organization's software reliably operates the electronic records system and processes its data;

h) system changes: a record of changes and alterations is kept;

i) privacy: the use of the data in the organization's electronic records complies with the relevant Canadian, provincial and territorial privacy statutes governing the collection, use or disclosure of personal information, confidential commercial information, trade secrets, privileges or other confidential information; and

j) security: security procedures, such as protection against unauthorized access and disaster recovery plans, are used to guarantee the integrity of the electronic records system.

Proof of these factors is provided by the Records management manual (see 6.4) and the IT system management guide (Section 7).

5.3 Electronic discovery (e-discovery) and litigation preparedness

Electronic discovery is a pre-trial procedure in civil litigation requiring an exchange of relevant electronic records, that may include metadata, among the parties. Investigations and inquiries also involve the collection and production of electronic records, sometimes in very large numbers. There is a parallel system to civil law discovery for disclosure in criminal law proceedings involving pre-trial applications, the preliminary inquiry and *voir dire* hearings held during trial. The huge volumes, varying formats and volatility of electronic records present a number of challenges.

The first challenge is the identification of potential sources of relevant information. Organizations with a well-managed electronic records system will be able to find, preserve and collect relevant records much more quickly, accurately and cost-effectively than those whose electronic records are disorganized. As a result, electronic records management should be in place long before the need to perform e-discovery arises. A second challenge, in terms of time and expense, is record review and processing of records, which is increasingly being done using automated computer systems. More and more, e-discovery requires the review of thousands of records for relevancy and privilege. This review is increasingly being done with the assistance of machine learning (Technology-Assisted Review, or TAR, see 5.3.1). Organizations that are in a position to efficiently collect only those records that are relevant (for example, by record type, record date, author/recipient or subject matter), will benefit from the reduced cost of review. A third challenge is for organizations to produce the relevant electronic records required by the court so that these records can be admissible as evidence in the legal proceedings. For more information on e-discovery in civil litigation, refer to the Sedona Canada Principles (see footnote 1). For disclosure in criminal law proceedings, see R. v. Oler, 2014 ABPC 130 (CanLII).

5.3.1 Technology-Assisted Review and other automated tools and techniques

Organizations may require their legal team and Record Officer (RO) to use Technology-Assisted Review (TAR) to meet the requirements of e-discovery. Methods using TAR are varied and may include: probabilistic search models, based on word interrelationships, proximity, and frequency; fuzzy search models, based on the core component of each word to capture all its possible forms; cluster search models, based on examination of groups of documents having similar content; and search categorization models that rely on a thesaurus. The TAR applications are equally varied, ranging from autocategorization systems, de-duplication systems, email threading and predictive coding, to visual analysis.

However, courts may differ in their opinions as to the accuracy of such devices. For information on how to conduct e-discovery using TAR, see the *Sedona Canada Principles.*

5.4 Legal hold

A legal hold is an obligation to preserve recorded information and arises as soon as litigation is contemplated or threatened.[1] However, as to when that point is reached is an issue requiring legal advice. It can be difficult to assess in the early stages of a dispute. Such steps taken too early may involve disproportionate cost and effort. But delay in imposing a legal hold upon normal disposal procedures can result in evidence being lost and consequently, penalties for spoliation. Therefore, a "good faith" assessment, based upon legal advice, should be carried out.

Notice of the need to impose a legal hold by preserving records in both paper and electronic form, shall be given to all affected parties, including relevant non-parties and the organization's IT and records management staff. Such notice shall provide clear instructions and details regarding the kinds of information that shall be preserved. Records custodians shall be informed when such preservation requirements are lifted.

The records system shall have the capability to suspend the disposition of records (and all other recorded information) subject to a legal hold, audit, review, investigation, inquiry, access to information request or other legal or administrative proceeding. The RO, in consultation with the legal adviser, IT, and business managers, shall develop and implement a detailed, written legal hold procedure that defines among other things:

a) the individual or position within the organization who is authorized to issue, modify, and rescind a legal hold;

b) the process of co-ordination with the organization's legal advisers;

c) the process for managing the legal hold and ensuring compliance;

d) the process by which custodians and data sources will be appropriately identified;

e) the IT systems vital to the legal hold;

f) the protection of the records from unauthorized access or modification; and

g) the actions taken to document the legal hold process.

The procedure shall include staff training on how to implement and manage the legal hold, and administer it without attracting sanctions for spoliation. The procedure shall emphasize that courts have a number of options to sanction a party which spoliates relevant evidence. These can include:

a) order the detention, custody, or preservation of evidence;

---

[1] Sedona Canada Principles is the title of a project of the Sedona Conference Working Group 7, Sedona Canada. "Sedona" is a reference to Sedona, Arizona, where the Sedona Conference is located. A pdf copy of The Sedona Canada Principles may be downloaded from Sedona Canada Principles site at https://thesedonaconference.org/node/9995. Principle 3 of the *Sedona Canada Principles* states: "As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information."

b) draw an adverse inference against a party guilty of spoliation;

c) refuse to admit evidence;

d) refuse to hear witnesses;

e) refuse to permit a party to examine or cross-examine a witness;

f) levy court costs against a spoliator;

g) impose a contempt of court order upon a spoliator; or

h) impose default judgment or dismiss the case (the court action).

Where there is concern that relevant evidence will not be preserved, a court can order that a party to legal proceedings be allowed to copy or take custody of evidence in the possession of another party.[2]

For these reasons, legal hold is potentially the responsibility of every individual within the organization.

5.5 Signatures

5.5.1 Electronic signature

Provisions of the CEA and the PIPEDA govern the use of electronic signatures in federal law. There are comparable provisions in the laws of the provinces and territories for electronic signatures. The function of a signature — to link a person with a document — is the same for a signature on paper or a signature associated with an electronic document. The requirement for a signature by a person is satisfied if the method used uniquely identifies the person and indicates the person's approval of the electronic record, and if the method used is reliable and appropriate in all the circumstances and includes agreement among the parties. It is generally accepted that "approval" means only willingness to adopt the text as one's own, without necessarily restricting a signature to one used to assent to a contract. Therefore, an "electronic signature" can mean electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with, the document.

Under PIPEDA, a secure electronic signature (digital signature) means an electronic signature that results from the application of a technology or process which it can be proved that:

a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;

b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;

c) the technology or process can be used to identify the person using the technology or process; and

d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.[3]

---

[2] Such a court order is called an "Anton Piller order." It is used for example, "when it is essential that the plaintiff should have inspection so that justice can be done between the parties... [and] there is a grave danger that vital evidence will be destroyed." In https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/2309/index.do, [2006] 2 S.C.R. 189, 2006 SCC 36, the Supreme Court of Canada provided guidelines for the granting and execution of Anton Piller orders.

[3] See s. 48(2) of the PIPEDA and its *Secure Electronic Signature Regulations* (SOR/2005-30). See also s. 31.8 of the CEA.

5.5.2 Wet signature

Where there is a requirement to maintain records with wet signatures (i.e. signatures made on the physical document using physical means) to provide evidence of approval, authorization, acknowledgement, verification, notarization or the witnessing of an act, such requirement can be satisfied by digitizing the record and maintaining a digital image of it, provided that all of the conditions set out for the digitization of paper records have been met. Because the legal, management, and technical information provided by this standard is general, users should seek expert advice before applying its recommendations to a specific records or IT system.

5.6 Authenticated paper copies for legal proceedings

Whenever paper copies of electronic records need to be produced, they shall be authenticated as true copies of the electronic records to support their admissibility and weight as evidence in legal proceedings. The procedures for producing and authenticating paper copies shall be documented.

The procedure for producing a paper copy of an electronic record shall require the use of an authorized individual's signature to authenticate the paper copy and to provide proof of authenticity when required to do so. Where the paper copy differs in structure, form, or content from the electronic record, the nature of the differences, their causes, and the manner in which they occur shall be documented in the authentication record (e.g. affidavit).

6 Records management program

6.1 General

A records management (RM) program is designed to support the creation, management, use, disposition and preservation of trustworthy records. The records management concepts, principles, methods and practices adopted by the organization shall demonstrate that an appropriate RM program is in place and is an integral part of the organization's usual and ordinary course of business.

The RM program shall support a records system consisting of appropriate records procedures and controls that complement business operating procedures. An organization shall

a) establish the RM program;

b) develop a RM policy, with definitions and assignment of responsibilities;

c) design RM procedures and related documentation;

d) select and implement technologies supporting the records system;

e) establish records protection measures, including audit trails and backup; and

f) establish a records quality assurance process.

6.2 Establishment of the RM program

6.2.1 Authorization

An organization shall authorize by a formal instrument (e.g. policy, directive, executive order, bylaw) the creation of a records management program, including a manual detailing its records system and setting out the policies, roles and responsibilities, and procedures for records creation, maintenance and disposition. The authorization shall reference the legislative authority and responsibilities of the organization with regard to the RM program, shall confirm that the RM program forms part of the organization's usual and ordinary course of business, and shall state that the RM program controls in an integrated way both electronic and hard-copy records. In addition to designating

an individual or position as the appropriate signing officer or authority (i.e., RO), the authorization shall articulate the following:

a) legislative authority and responsibility of the organization to create a RM program;

b) purpose of the RM program;

c) extent of the RM program (i.e., ownership, custody, control, and applicability), and any exclusions;

d) means of implementation of the RM program (i.e., designation of responsibilities);

e) required RM procedures (i.e., records creation, management, use, destruction/transfer or preservation);

f) required quality assurance that certifies that all RM duties are appropriately fulfilled; and

g) authorization for any changes or revisions to its RM program.

6.2.2 Responsibility

The role of the RO shall be clearly defined in the organization's formal authorization instrument (e.g., policy, directive) as responsible for implementing the RM program as an integral part of the organization's usual and ordinary course of business. The organization shall identify any other responsibilities to be assigned to the RO and other individuals or positions to ensure compliance with the RM program (e.g., an IT systems Security Officer [SO] responsible for ensuring IT system integrity).

6.2.2.1 Delegation of responsibility

An organization may delegate all or part of its RM program to an authorized third party (e.g. an external service provider). In any delegation, the roles and responsibilities of the authorized third party shall be clearly specified and documented to ensure that the trustworthiness of the electronic records is not compromised.

6.2.2.2 External service providers

The Canadian government does not prohibit government institutions under the *Privacy Act* or organizations under the *Personal Information Protection and Electronic Documents Act* from using an external service provider that stores personal information outside Canada. However, some provinces dictate that public bodies ensure that personal information under their care or control is stored and accessed only in Canada subject to legislative exceptions. As a result, organizations shall consult competent legal or other professionals to ensure compliance with the applicable law.

Where an organization uses an external service provider to carry out all or part of a RM program, the external service provider shall comply with applicable legal and regulatory requirements in the relevant jurisdictions that apply to its recorded information as well as the organization's RM policy and procedures. These provisions shall be included in any contractual document or service standards.

6.2.2.3 Use of external service provider services

In the contract, the detailing of procedures, processes and practices shall cover any type of service, including facilities management and electronic records storage, conversion and migration, and security. The contract is intended to ensure that the external service provider complies with the organization's policy, procedures, processes and practices. The organization shall hold a copy of, or have access to, the external service provider's proof of compliance and the effectiveness and security of the service.

The organization shall ensure that the external service provider signs a confidentiality and privacy protection agreement or is otherwise contractually bound to protect the organization from any breach of confidentiality or

privacy. Organizations shall ensure through contractual agreements that they will be immediately notified in the event of any access breach. The agreement shall also include provisions related to discontinuing access for terminated or otherwise suspended employees.

The agreement with the provider shall ensure that the organization's retention and disposition requirements and procedures are implemented and that records are protected, preserved and destroyed as directed. The agreement shall also ensure that if litigation, audit, or government investigations occur, or are expected to occur, regularly scheduled destructions of related records are immediately suspended and that the assigned retention period is resumed once the hold is no longer required.

6.3 RM policy

6.3.1 Requirement for a RM policy

An organization shall have a formal instrument (hereinafter "RM policy") stating that the management of electronic records is an integral part of its usual and ordinary course of business.

In some environments, it is useful to combine the RM program authorization and policy into one formal instrument.

6.3.2 Content of the RM policy

The RM policy shall contain statements to:

a) identify the records and the records system covered under the formal instrument (i.e., policy or bylaw), and any exclusions;

b) identify relevant RM, business, and IT standards;

c) establish the position of RO having responsibility for the records system or give authoritative recognition from senior management to an existing position with the same responsibility;

d) require that the records system comply with the RM manual, the law, and national and industry standards so that the system will always produce and/or store records admissible as evidence;

e) grant the RO the responsibility to maintain and amend the RM manual with the support of IT staff so that it continuously reflects the exact state of the records system and can stand as evidence of the system's compliance with the law and this standard;

f) list the high-level requirements for records creation, management, use, destruction/transfer or preservation;

g) ensure that IT staff works with the RO to integrate records management into the organization's usual and ordinary course of business, and to maintain that integration; and

h) identify the RO responsibilities with respect to records quality assurance and for monitoring compliance with the support of IT staff.

6.3.3 Compliance with the RM policy

Compliance with the policy requires the following:

a) authorization of the person (individual or position) responsible for obtaining and maintaining such compliance;

b) identification of the relevant legislation, directives and regulations that the organization shall comply with;

c) identification of any relevant national or international standards or part thereof that the organization shall comply with; and

d) assessment of how the organization complies with all applicable directives, legislation and regulations.

The above documents shall be noted in the RM policy. Periodic audits shall be conducted to verify compliance.

6.4 RM manual

6.4.1 General

The implementation of a RM program requires the use of a RM manual that consolidates all records related procedures to ensure consistency and completeness. The RM manual shall be consistent with the RM policy and any identified standards.

The RM manual shall describe the procedures for making, receiving, capturing, managing, using, protecting, destroying, and preserving records through their lifecycle. Changes to the RM procedures shall be authorized, documented, disseminated, and included in the manual.

The RM manual shall be kept up-to-date and accurately reflect the exact nature, functions, procedures and processes of the organization's records system, i.e., the way in which this system participates in and supports the usual and ordinary course of business, and the way in which the rapid change of technology impacts procedures and processes.

The RM manual shall specify the operation and use of the records system and include references to other relevant documentation (e.g., other procedure manuals, business procedures, IT system documentation) as appropriate. The RM manual shall have a formal review cycle to ensure ongoing alignment with other organizational requirements.

6.4.2 Records capture

6.4.2.1 General

Records may be generated by the organization or imported into the records system from an external source. The RM manual shall document control procedures for capture, and quality assurance levels for accuracy and completeness of records and their metadata. The RM manual shall document procedures for records in any form, including non-textual records (e.g. audio, images, video and multimedia).

The RM manual shall specify procedures enabling implementation of systematic version controls for all records. Responsibility and procedures for replacing stored records with new versions shall be documented in the system documentation. A record version control-procedure shall be established for all records.

Where workflow systems are implemented, operational details and change-control procedures shall be documented in the RM manual. Such details should ensure that record integrity will not be compromised during a workflow process and records will not be lost.

6.4.2.2 Metadata

Metadata are attributes that identify the content, context, and structure of records and describe their use, management, custodial history, and technological changes.

There is no legal minimum set of metadata required for electronic evidence to be admitted in legal proceedings in Canada and given weight as documentary evidence. Metadata are managed by Canadian courts on a case-by-case basis. However, metadata creation and management is an integral part of records management, enabling identification, registration, classification, access and discovery, disposition, preservation, proof of integrity and

authenticity, version control, etc. Metadata ensure the authenticity (identity and integrity), reliability, and usability of records over time.

The production, management, disposition, and preservation of metadata should be formally mandated by the organization in its RM manual. The RM manual should identify that metadata:

a) consists of information about records, regardless of medium, that is used to identify, describe, manage, authenticate, access, understand, and interpret those records;

b) is produced at the time of records creation (i.e., when a record is made or received or stored to an aggregation of records) and continues to accumulate over the record's lifecycle;

c) is an integral part of a record, and its production and management forms an integral part of the records system;

d) is kept and used in the usual and ordinary course of business by the records creator and is discoverable;

e) may include personal information, and be subject to privacy law; and

f) supports the assessment of its trustworthiness, that is, its reliability, accuracy and authenticity as evidence.

Metadata shall be captured or created that uniquely identify a record and establish its integrity at the time of creation and throughout the records lifecycle. Critical metadata includes, but is not limited to, elements such as document title, dates of creation and/or modification, author, recipient, document type, etc. Metadata shall continue to accrue or be created that tracks technological changes (migration, conversion, etc.), integrity, rights (permissions, access), etc.

6.4.2.3 Digitization

Digitization is a process whereby organizations convert records from analogue to digital form. Since many records are now created, captured, maintained, used, and preserved in digital form, an organization may choose to digitize analogue records to reduce retrieval efforts and/or develop end-to-end digital workflows. Digitization may also reduce requirements for physical storage and/or improve business continuity. While digitized records are accepted in court, physical records may at times be viewed as best evidence due to their status as originals.

An organization may choose to digitize recorded information on-premises and/or outsource digitization to external service providers. On-premises digitization may be centrally managed and involve specialized equipment operated by trained technicians or distributed across an organization with employees using multi-function devices or desktop scanners to produce digitized records. Regardless, all digitization processes shall be carefully aligned to business needs and designed to create sufficiently high-quality digital substitutes of analogue records, with minimal, identifiable and acceptable levels of loss of information or other detail as determined by the organization. An organization shall be able to attest that the digital versions of the analogue records are complete and accurate, and thus capable of providing evidence of the activities in which the source records participated. Further, the digital versions shall be discoverable and available to those with the right to access them for as long as they are required.

Prior to initiating a digitization project, an organization shall:

a) assess whether records are appropriate candidates for digitization;

b) ensure there are no legal barriers to replacing analogue records with digital records;

c) determine whether all or a selection of the records should be digitized;

d) ensure sufficient labour resources, equipment, and funds, are available for project completion;

e) determine whether digitization should be done on-premises or contracted to an external service provider;

f) designate either the analogue or the digitized record as the official record; and

g) determine whether the source records will be retained or destroyed.

The RM manual shall outline the processes and procedures that result in complete and accurate reproductions of source records, along with appropriate metadata for the management and retrieval. Quality assurance shall be conducted and certified by the organization, and source records shall not be subject to authorized destruction until all quality assurance procedures and all corrections are completed.

The RM manual shall contain a listing of analogue records approved by the organization for digitization and the legal and business rationales for authorized destruction of any source records. If paper records are routinely destroyed following digitization, digitized copies become authentic and authoritative records, which can be used for business transactions and legal purposes. Their authenticity, reliability and integrity is confirmed through adherence to the digitization requirements of the RM manual and the integrity of the system where the digitized records are stored and managed (see s. 31.1 and s. 31.5 of the CEA).

6.4.3 Classification and indexing

Classification and indexing are key components of every RM program in that they allow for a logical organization of records, and for their identification, control, retrieval and disposition. All records should be classified in order to fix them into their documentary context, and indexed in order to facilitate their retrieval. With electronic records, these functions are implemented through metadata. It is required that the following be clearly outlined in the RM manual:

a) the specification of the classification methodology used (e.g. functional classification) and a representation of the classification system by means of a schema;

b) type and structure of indexing used, including the primary index element as well as all additional levels of indexing;

c) procedures for updating classification schema and index;

d) procedures for amending inaccurate classes, codes, or index terms;

e) procedures for implementing c) and d);

f) methods for tracking updated, deleted or destroyed status of classification codes and indexing terms; and

g) procedures for performing quality assurance of classification and indexing.

6.4.4 Records maintenance and use

The RO shall oversee and coordinate all the activities associated with ensuring the records in the records system remain authentic, available, and secure.

The RO shall maintain a record of the authority to retrieve, read, annotate, edit, transmit and delete records (i.e. access privileges), granted to officers and employees of the organization. The RO shall ensure that the nature of any action undertaken upon the records is documented, whether through additions of integrity metadata or by compilations of reports, to provide an audit trail (see 6.5.5) of what has happened to the records since their creation. Such information is necessary when assessing the ongoing trustworthiness of the records in the system.

6.4.5 Records retention requirements

The time period for which records shall be retained shall be determined by authorized individuals or positions within an organization, including those responsible for the organizational functions that the records support, i.e., the legal adviser (to ensure compliance with legislation), the financial officer (to ensure compliance with financial requirements),

and the RO (to ensure that retention and disposition decisions are based on sound records management and preservation principles and methods). Record retention requirements shall be documented in the organization's records retention schedule, which should be linked to the records classification schema. The assignment of the responsibility for identification of records retention requirements to authorized individuals or positions (e.g., the RO) shall be formally documented.

Retention periods are usually based on the value of the records and the organization's need to access as well as evidentiary, risk management, legal and audit requirements. It is the responsibility of the organization's RO to ensure that a proper appraisal of the records is conducted based on

a) how the records are used by the organization (internally and externally);

b) users' needs for access to the records in the event of a disaster;

c) financial, legal, social, political, historical value of the records;

d) costs/benefit analysis of records retention;

e) impact on the organization if the records are destroyed; and

f) evidentiary capacity of the records in the event of litigation, audit or investigation.

After the value of each set (class or category) of records has been identified, then the RO shall document the length of time to retain the records, and how to transfer them to the designated custodian (for either a determined period of time or permanent retention), or how to destroy them after they are no longer required.

Whether an organization will need to keep the records for short or long periods or indefinitely, the organization shall ensure that the technological environment is able to support any such retention (e.g. fixed-date or event-based retention, or permanent retention). Furthermore, before any disposal decision (be it destruction or transfer) is implemented, it shall be reviewed by the RO, in case legal hold is required (see 5.4) or an event has occurred that involves a longer retention period.

The organization's records management policy shall also define "transitory records", records to which no retention requirement applies and which have no enduring value in documenting or supporting the organization's business.

6.4.6 Records disposition

6.4.6.1 General

Disposition refers to the action taken on records after the expiration of the records retention period: destruction or transfer. Conducted in compliance with a records retention and disposition schedule, records disposition is regarded as an integral part of an organization's usual and ordinary course of business. The RM manual shall prescribe that all dispositions be documented. The RO shall be given the authority to suspend the destruction or transfer of records subject to legal hold (see 5.4), organizational or government review or audit.

6.4.6.2 Disposition process

The RM manual shall require that records disposition occur after the appropriate retention period has expired, disposition has been authorized, and any barrier to elimination has been removed. The organization shall be capable of submitting documentation of the disposition of its records when proof is warranted or required, based on business, legal or audit requirements. This documentation should identify the records disposed of using the associated metadata (e.g., the classification code, inclusive dates, office of primary responsibility), the organization who authorized the disposition, and the time of disposition. This record of disposition actions shall be kept as proof by the organization for as long as the organization exists.

The RM manual may require that metadata be retained after the records they relate to have been disposed of; the metadata should then record the event of disposition. If an electronic record is associated with more than one aggregation of records, it may be disposed of in the context of one aggregation and retained in the context of another; in this case the disposition is carried out by deleting from the record metadata associated with the set of records that is disposed of.

6.4.6.3 Destruction of electronic records

System transaction logs, audit trails and other appropriate records of destruction and amendment activities may need to be retained permanently. It may be required to destroy a specific record from a records system because of legal or administrative requirements, particularly in accordance with privacy regulations or other legislation. The RM manual shall allow the records system to destroy, amend or correct records using an editable process. For destroyed records, the system procedures shall ensure that both the record and the record locator are destroyed. The destruction of electronic records needs to be completed in such a way that the confidentiality of the records is preserved, and personal information is not disclosed.

6.4.6.4 Transfer of electronic records to another organization

The RM manual shall require that records transferred to and accepted into custody by a designated custodian (e.g., an archives) appear in the documentation of both the transferring and the receiving body. It may also require the identification of the hardware and software that generated the records, and the program documentation that describes the format, file codes, file layout and other technical details about the records system in which the records resided.

6.4.7 Records preservation

The RM manual shall recognize that, in the digital environment, preservation begins with the controlled creation and maintenance of records in preservable file formats, with the essential identity and recordkeeping metadata required to demonstrate that a record was made or received or stored in the usual and ordinary course of business, is authentic, and has been properly maintained in the records system without unauthorized modifications.

An organization’s records system shall have the ability to permanently retain those records whose value to the creator is enduring. Records created by organizations may have enduring value and qualify for permanent preservation, and shall be safeguarded against software obsolescence.

6.4.7.1 Records conversion and migration

The RM manual shall provide guidance on conversion and migration. Records conversion and migration are methods used to overcome software obsolescence, which results in the inaccessibility of electronic records over time. There are two kinds of digital record obsolescence: file format obsolescence, where available software applications can no longer open or view the contents of a digital record; and system obsolescence, when a system or application is no longer supported (in some cases due to hardware obsolescence) and the records cannot be retrieved, opened, or viewed. File format obsolescence shall be addressed by file conversion, that is, by moving a record from one file format to another (the native application or source file should also be maintained). System obsolescence shall be addressed either by migrating digital files to a new system or application (often leveraging system virtualization), or, in rare cases, keeping the old hardware or buying specialized software to access obsolete media.

Conversion and migration always involve risk, and, before undertaking them, the organization shall identify the required functionalities of the old format and those that have to be maintained in the new format and system, and document such decisions, as different software may render the same record in different ways. Regardless of the preservation format that is chosen, both conversion and migration shall be integrated in a well-documented business process that is part of the regular operation of the records system.

Organizations shall have a conversion and migration policy, and the RM manual shall outline detailed procedures ensuring that records’ structure, content, identity and recordkeeping metadata, and, in the case of email, attachments,

links, proof of delivery, distribution lists, and relationship to other records of the organization within and outside the organization are protected and preserved. The integrity of each file should be verified after conversion or migration in order to identify and correct any errors.

6.4.7.2 Preservation formats

The RM manual shall identify the organization's preferred formats for preservation by type of record. A variety of resources exists to aid organizations in selecting the proper preservation formats for their records and carrying out the conversion. The decision on the preservation format shall be based on how much change can be introduced before the record representation becomes too degraded to serve as a reliable copy of the record in its native format in a legal proceeding.

6.4.8 Quality assurance

In essence, a records management program is a quality assurance program designed to support the creation, management, use, disposition, and preservation of trustworthy records that provide evidence of an organization's activities in the usual and ordinary course of business. While the records management policy and manual documents the controls that the organization has put in place to support record and system integrity, quality assurance is required to ensure that the organization's records management program is compliant and meets legislative, administrative, operational, and technical requirements on an on-going basis and that any fraud or abuse is either avoided or uncovered and addressed at the earliest juncture.

Quality assurance means that the organization defines the appropriate level of service, and ensures staff understand their roles and responsibilities and are trained to provide this level of service. To this end, the RO shall implement appropriate quality assurance processes, including, but not limited to, performance and compliance monitoring, self-assessment and external audits, incident handling, and record and certify that all RM duties are fulfilled. The RO shall immediately report all significant issues to the senior executive in charge of the program who shall respond as required and direct and/or approve necessary RM program adjustments.

7 IT system management

7.1 General

All significant details of the logical and physical architecture of the IT system keeping the records shall be fully documented in an IT system management guide, including the responsibilities and the relationships between IT system management, the RM program, and the conduct of the organization's business. The IT system management guide shall be structured so that the integrity of the system can be demonstrated for any point in time.

The documentation required for the IT system shall include the following:

a) description of the hardware, and network elements of the system and how they interact;

b) description of operating systems and application software, including record formats;

c) description of IT security protections such as firewalls, system backups, and disaster recovery;

d) description of system integrity verification procedures, including event scheduling and accountabilities, for monitoring and maintaining systems and data integrity and for taking preventive and corrective action where required;

e) trouble logs, schedules and procedures for assessing the system's ongoing operational integrity and for taking corrective action where required;

f) impact and risk assessment of system and data integrity following sudden, infrequent technical problems or disaster in the functioning of the records system or its related IT system, when they do not operate as per their intended design and specifications;

g) documentation of changes to the system, including risk and impact assessment on system and data integrity, including all responsible individuals or positions and a full account of the processes and activities undertaken to affect the change; and

h) procedures to control the use of system maintenance hardware and software that can bypass system access controls, and necessary authorizations for their use.

The manager responsible for the IT system shall ensure that the IT system management guide is kept up to date.

7.2 Technology risk assessment

Increasingly, organizations are creating, managing, and using records in a variety of systems, services, and devices. Recorded information may be accessible from anywhere, and subject to security challenges including but not limited to being used out of context, copied, revised, manipulated, hacked or otherwise tampered with. As a result, the benefits and risks of adopting these shall be established through a process of risk assessment.

A risk assessment process provides a mechanism for identifying, classifying, and weighing risk and for developing risk mitigation strategies and policies, especially those associated with new technologies. The organization shall consider the complex legal implications of a new technology using a multi-disciplinary approach (e.g. legal, security, privacy, IT, risk management, etc.) that takes into account the organization's existing infrastructure and risk tolerance.

Prior to commencing the adoption of any technology, the organization shall:

a) establish a risk assessment team (i.e. risk manager, IT enterprise architect, IT network analyst, legal expert, SO and RO) to consider the new technology and make recommendations on adoption;

b) reference the organization's existing risk management framework (i.e. policy, procedures, and guidelines);

c) identify stakeholders and use cases;

d) identify, assess and mitigate threats and risks associated with the technology;

e) ensure reporting mechanisms to senior management are in place, and that senior management has made their determination prior to adoption;

f) develop policy and documented procedures (including updating the RM manual and IT system management guide); and

g) communicate policy and procedures to staff.

In provincial jurisdictions where government institutions are subject to privacy impact assessment requirements, the risk assessment and privacy impact assessment processes may be combined.

Technologies that require a careful risk assessment include, but are not limited to, mobile devices, social media platforms, artificial intelligence and automated decision systems.

7.2.1 Mobile devices

Organizations that allow employees to use their own devices in the execution of their duties shall conduct a risk assessment to consider issues arising from the "borderless" nature of personal and professional use including, but not limited to, database and software licensing, security, privacy, intellectual property, and employment law.

Following a risk assessment, the organization shall provide a clearly articulated and enforceable policy about the use of personal devices including:

a) if personal devices are allowed for work activity;

b) what types of devices are allowed;

c) what are the employer/employee responsibilities with respect to use, including if/when the employee leaves the organization; and

d) how work records will be managed and transferred to the organization's record keeping system.

7.2.2 Social media

When an organization uses social media, there are issues from an evidentiary point of view, notably:

a) the identification of records;

b) the determination of their author, and owner (necessary in order to establish who has a duty to identify, capture and manage the record);

c) the definition of their context (and therefore the ability to determine whether they are generated in the usual and ordinary course of business);

d) the assessment of their reliability, accuracy and authenticity; and

e) the identification of a chain of custody (particularly if individuals upload business records to their own social media pages or those of others).

Organizations shall develop a social media policy that defines:

a) when a posting is considered to be a record; and

b) the process through which records are captured, including the creation of an authentic copy with identity metadata that clearly indicates the context of the posting, the responsibility for it, and any related actions.

Existing records of the organization that are posted on social media as links shall be maintained by the organization in accordance with the existing classification, index, and retention and disposition schedules, taking into consideration that social media providers retain such records indefinitely.

When the possibility of litigation arises or is anticipated, it may be necessary to take additional snapshots or images of relevant material, since social media sites can be shut down, accounts or memberships terminated, and content deleted.

7.2.3 Artificial intelligence and automated decision systems

Records are increasingly being created, accessed, used, and analyzed using complex artificial intelligence (AI) systems and automated decision systems (ADS). Regulation of AI systems in Canada is still developing.[4]

[4] High-level aspirational principles outlined in the https://www.montrealdeclaration-responsibleai.com/the-declaration (2018, Université de Montréal). Further guidance is found in the https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (2019, Treasury Board of Canada). The first law that would create new rules for the responsible development and deployment of artificial intelligence (AI) in Canada, Bill C 27 (The Digital Charter Implementation Act, including the Artificial Intelligence and Data Act) was introduced on June 16, 2022.

Legal and ethical issues to consider when using AI systems include but are not limited to:

a) bias (data, algorithmic, human);

b) lack of transparency of AI systems and processes, including how the AI systems were trained;

c) lack of explainability of AI systems and processes, including how the AI systems were trained;

d) data privacy and security;

e) relevance of AI records as documentary evidence; and

f) authenticity, integrity, validity of AI records or results.

If an organization uses AI or ADS, it should conduct a risk assessment and determine how it will prove that the AI/ADS system produces results that can be shown to be accurate, and reliable (i.e., consistent).

7.3 Backup and system recovery

Effective procedures for the backup of electronic records and all associated information (e.g., index files and audit trails) as well as those for system recovery shall be included in the IT system management guide. Only authorized individuals shall be allowed to enable or disable the backup and recovery functions.

The IT system management guide shall require that the storage media be tested to prove that no recorded information or metadata have been lost or overwritten, and that backups be tested at predetermined intervals for accuracy and integrity.

A backup log shall be kept in the system's audit trail of all backup and recovery activities, including any problems incurred during the procedure. It is prudent to have several simultaneous backup copies of recorded information and application programs and to maintain one of these at another location. The IT system management guide shall include the procedures for moving a backup copy to and from an off-site facility.

If the structure of the data files held on a backup copy differs from that of the electronic records, the differences shall be documented.

The IT system management guide shall require that, where backup data files are used to recover from a system failure, procedures shall be documented to ensure that data file integrity has not been compromised. It shall also require that backup procedures and details about transfers shall be retained for as long as the referring records are required.

The technological aspects of backup and system recovery shall be covered by the IT system management guide. Mirroring and redundancy can substitute backup for system recovery in case of a disaster.

Backups are a product of the security function of an organization and should be regularly disposed of on a rotational basis according to an explicitly defined term.

7.4 Security and protection

7.4.1 IT security policy and procedures

An organization shall have an IT security policy specifying the levels of access to the records system (i.e., the whole of an organization's records and associated records management and preservation systems), as well as the levels of protection applied to the IT system (i.e., the whole of an organization's computers, software, and devices used to process and transform information).

Procedures shall be implemented in accordance with the organization's IT security policy. These procedures shall include a system-wide definition of user authentication and permission controls, privileged users, and notification of, and protection against, unauthorized access as well as guidelines on access and changes in personnel with access. Security screening of individuals working for the organization shall be in accordance with the information's level of sensitivity. The accommodation and operating environment for the storage, transportation and maintenance of storage media shall be in accordance with relevant national or international standards.

7.4.2 Encryption and secure electronic signatures

Where there is a requirement for the safeguarding of recorded information, encryption shall be used to improve the security and ensure the integrity of recorded information during transmission and storage.

Where secure electronic signatures are used, procedures shall be implemented for encryption key allocation and management and for certificate management. Encryption or electronic signature keys shall be valid, kept secure and made available only to authorized individuals.

7.4.3 Date and time stamps

The regular checking of computer system clocks for accuracy concerning date and time keeping shall be documented. Date-keeping and time-keeping involve the ability to detect and correct errors. All actions taken concerning error correction or resetting of system clocks on all computer systems and devices shall be documented.

An organization shall identify the individuals who are authorized to access and modify system clocks, and ensure that appropriate access control measures are established.

7.5 Audit trail

7.5.1 General

Audit data represents the history of each record and the associated metadata. Audit data is the definitive proof that certain events and transactions occurred. As such, the capture of audit data shall always be an ongoing process and audit data shall always be protected from alteration and loss. Audit data is collected into the audit trail.

Audit trails shall contain sufficient and necessary audit data to provide evidence of the authenticity of the records made by the organization and of the integrity of any received records from the moment of receipt. The audit trail of an IT system shall consist of system-generated and operator-generated logs containing data about capture of and changes to (e.g., modification, deletion, access) the records stored on the system. The integrity of the audit trail is important to satisfy the best evidence rule, as required by the electronic records provisions of the Evidence Acts, and for establishing the weight to be given to records (i.e., their probative value and persuasiveness as reliable records).

Procedures for audit trails shall be documented in the IT system management guide.

7.5.2 Management of audit trail records

The audit trail logs shall be subject to internal records management procedures similar to those for other essential records of the organization and shall be included as a specific document type in the IT system management guide. Audit trail data kept within the records system shall be made unalterable in the secure environment. Secure backup copies of the audit trail shall be kept.

7.5.3 Content of the audit trail

The organization shall establish the content of the audit trail.

The following are minimum content requirements:

a) identification of the recorded information to which the action was applied (including unique identifiers);

b) individual or position responsible for initiating and carrying out the action; and

c) date and time of events such as:

    1) initial capture of an electronic record or data element into the system;

    2) creation of new electronic record versions;

    3) creation, amendment and deletion of metadata;

    4) changes in access authorization for records or data;

    5) changes in retention and disposition requirements;

    6) assignment of a record security classification or changes to that classification; and

    7) modification, destruction or transfer of records or data.

7.5.4 Audit trail creation

Audit trail data shall be generated automatically by the IT system. If it does not happen, the procedures for generating audit trail data shall be documented in the IT system management guide. These procedures shall apply to the organization and any contracted external service providers.

For records selected for permanent preservation, the designated preserver shall have access to audit trail data in order to verify the authenticity of the records.

7.5.5 Access

Access procedures and authorizations to audit trail data shall be documented in the IT system management guide.

7.5.6 Audit trail of conversion and migration

If records are moved between storage devices as part of a conversion or migration process, details of the process shall be stored in the audit trail. Procedures for migration or conversion shall include methods for proving that any related metadata are also migrated or converted and be documented in the IT system management guide. Where records have been converted from one file format to another, details of the conversion shall be stored in the audit trail log.

7.5.7 Workflow

Where workflow systems exist, the IT system management guide shall define at which points in the workflow audit trail data shall be generated and kept in the IT system. In a typical workflow system, audit trail data are generated at each step in the workflow.

The audit trail data to be generated and kept may change as the workflow processes are changed.

The IT system shall permit an authorized individual to select the audit trail points for which audit trail data are generated.

7.5.8 Verification

Audit trail data shall be kept of activities or events that may need to be reconstructed in the future as additional evidence to support the evidentiary capacity of stored electronic records.

Annex A
(informative)
Sources for this standard

A.1 Introduction

This annex sets out the sources that have been considered for this standard.

CAN/CGSB-72.34 is based on the law of evidence for the admission of documents commonly referred to as documentary evidence. It focuses on those documents that the *Canada Evidence Act* regards as an exception to the hearsay rule, that is, business records. The law on this question is a mix of common law (laws developed through case decisions by judges, not enacted by legislative bodies) and statutes. The common law on documentary evidence is similar across Canada, in the common law jurisdictions. The statute law is found in the federal, provincial and territorial evidence acts, which vary slightly. The basic rules for Quebec are found in the *Civil Code of Quebec*, notably Book Seven on Evidence, and, in particular, articles 2837 to 2842, and 2870.

Today, the general law of documentary evidence is supplemented in much of Canada by specific legislation dealing with electronic documents or records.

The relevant federal statute is the *Canada Evidence Act* (CEA). It was amended in 2000 by Part 3 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which added sections 31.1 through 31.8 to the CEA.

A.2 Sources

The sources for this standard include:

a) Canadian legal requirements, including legislation and pursuant regulations (federal, provincial, territorial);

b) Information, communication, and technology (ICT) requirements and standards;

c) Business operation requirements and best practices (and related standards); and

d) Common operational requirements of organizations as well as best practices in records keeping, ensuring integrity of digital recorded information.

The committee of experts that drafted this standard is drawn from well-known Canadian professional and industry associations in the areas of records, information, and image management; legal and financial services; and accounting and auditing. The experts represent both user and supplier perspectives, ensuring a balanced approach.

Bibliography

These sources were reviewed and considered in the development of this standard; some are referenced in the guidance and other information sections in this standard.

American National Standards Institute (ANSI). ANSI/ARMA 18-2011 *Implications of Web-Based, Collaborative Technologies in Records Management.* Available from Standards Store by Accuris: https://global.ihs.com/.

American National Standards Institute (ANSI). ANSI/ARMA 19-2012 *Policy Design for Managing Electronic Messages.* Available from Standards Store by Accuris: https://global.ihs.com/.

ARMA International. *Implementing Electronic Messaging Policies* (2018). Available from: https://www.arma.org/.

ARMA International. *Guideline for Outsourcing Records Storage to the Cloud* (2010). Available from: https://www.arma.org/.

CSA Group. CAN/CSA ISO/IEC 11179-3:2013/Amd 1:2020 *Information technology — Metadata registries (MDR) — Part 3: Registry metamodel and basic attributes.* Available from: https://www.csagroup.org/.

CSA Group. CAN/CSA ISO/IEC 14662:10 (R2020) *Information technology — Open-edi reference model.* Available from: https://www.csagroup.org/.

International Organization for Standardization (ISO). ISO 13008:2022 *Information and documentation – Digital records conversion and migration process.* Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO 15489-1 *Information and documentation — Records management — Part 1: General.* Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO/TR 15801:2017 *Document management – Electronically stored information – Recommendations for trustworthiness and reliability*. Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO/IEC 15944-12:2020 *Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)*. Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO 19005-1 *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).* Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO 19005-2 *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).* Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO 19005-3 *Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3).* Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO 23081-1 *Information and documentation – Records management processes – Metadata for records – Part 1: Principles.* Available from Standards Store by Accuris: https:// global.ihs.com/.

International Organization for Standardization (ISO). ISO/IEC 27001 *Information technology – Security techniques – Information management systems – Requirements*. Available from Standards Store by Accuris: https://global.ihs.com/.

International Organization for Standardization (ISO). ISO/IEC 27002 *Information technology – Security techniques – Code of practice for security controls.* Available from Standards Store by AccurisStandards Store by Accuris: https:// global.ihs.com/.

International Organization for Standardization (ISO). ISO/IEC 27005 *Information technology – Security techniques – Information security risk management.* Available from Standards Store by AccurisStandards Store by Accuris: https://global.ihs.com/.

R. v. Oler, 2014 ABPC 130 (CanLII). Available from : https://ca.vlex.com/vid/r-v-oler-d-681435505.

The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery, Third Edition*, 23 SEDONA CONF.J. 161 (2022). Available from: https://thesedonaconference.org/publications.