Gouvernement du Canada
Government of Canada

Office des normes générales du Canada
Canadian General Standards Board

CAN/CGSB-72.34-2024

Remplace CAN/CGSB-72.34-2017
Confirmée, mars 2022

Enregistrements électroniques utilisés à titre de preuves documentaires

Office des normes générales du Canada ONGC

CCN SCC

Canada

Expérience et excellence
Experience and excellence
ONGC CGSB

Énoncé de l'Office des normes générales du Canada

La présente norme a été élaborée sous les auspices de l'OFFICE DES NORMES GÉNÉRALES DU CANADA (ONGC), qui est un organisme relevant de Services publics et Approvisionnement Canada. L'ONGC participe à la production de normes facultatives dans une gamme étendue de domaines, par l'entremise de ses comités des normes qui se prononcent par consensus. Les comités des normes sont composés de représentants des groupes intéressés, notamment les producteurs, les consommateurs et autres utilisateurs, les détaillants, les gouvernements, les institutions d'enseignement, les associations techniques, professionnelles et commerciales ainsi que les organismes de recherche et d'essai. Chaque norme est élaborée avec l'accord de tous les représentants.

Le Conseil canadien des normes a conféré à l'ONGC le titre d'organisme d'élaboration de normes national. En conséquence, les normes que l'Office élabore et soumet à titre de Normes nationales du Canada se conforment aux exigences et lignes directrices établies à cette fin par le Conseil canadien des normes. Outre la publication de normes nationales, l'ONGC rédige également d'autres documents normatifs qui répondent à des besoins particuliers, à la demande de plusieurs organismes tant du secteur privé que du secteur public. Les normes de l'ONGC et les normes nationales de l'ONGC sont élaborées conformément aux politiques énoncées dans le Manuel des politiques et des procédures pour l'élaboration et le maintien des normes de l'ONGC.

Étant donné l'évolution technique, les normes de l'ONGC font l'objet de révisions périodiques. L'ONGC entreprendra le réexamen de la présente norme et la publiera dans un délai qui n'excédera pas cinq ans suivant la date de publication. Toutes les suggestions susceptibles d'en améliorer la teneur sont accueillies avec grand intérêt et portées à l'attention des comités des normes concernés. Les changements apportés aux normes peuvent faire l'objet de modificatifs ou être incorporés dans les nouvelles éditions des normes.

Une liste à jour des normes de l'ONGC comprenant des renseignements sur les normes récentes et les derniers modificatifs parus, figure au Catalogue de l'ONGC disponible sur le site Web suivant www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html, ainsi que des renseignements supplémentaires sur les produits et les services de l'ONGC.

Même si l'objet de la présente norme précise l'application première que l'on peut en faire, il faut cependant remarquer qu'il incombe à l'utilisateur, au tout premier chef, de décider si la norme peut servir aux fins qu'il envisage.

La mise à l'essai et l'évaluation d'un produit ou service en regard de la présente norme peuvent nécessiter l'emploi de matériaux et/ou d'équipement susceptibles d'être dangereux. Le présent document n'entend pas traiter de tous les aspects liés à la sécurité de son utilisation. Il appartient à l'usager de la norme de se renseigner auprès des autorités compétentes et d'adopter des pratiques de santé et de sécurité conformes aux règlements applicables avant de l'utiliser. L'ONGC n'assume ni n'accepte aucune responsabilité pour les blessures ou les dommages qui pourraient survenir pendant les essais, peu importe l'endroit où ceux-ci sont effectués.

Il faut noter qu'il est possible que certains éléments de la présente norme soient assujettis à des droits conférés à un brevet. L'ONGC ne peut être tenu responsable de nommer un ou tous les droits conférés à un brevet. Les utilisateurs de la norme sont informés de façon personnelle qu'il leur revient entièrement de déterminer la validité des droits conférés à un brevet.

À des fins d'application, les normes sont considérées comme étant publiées la dernière journée du mois de leur date de publication.

Communiquez avec l'Office des normes générales du Canada

Pour de plus amples renseignements sur l'ONGC, ses services et ses normes ou pour obtenir des publications de l'ONGC, veuillez nous contacter :

sur le Web — http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html

par courriel — ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca

par téléphone — 1-800-665-2472

par la poste — Office des normes générales du Canada
140, rue O'Connor, Tour Est
Ottawa (Ontario) Canada K1A 0S5

Énoncé du Conseil canadien des normes

Une Norme nationale du Canada est une norme qui a été élaborée par un organisme d'élaboration de normes (OEN) titulaire de l'accréditation du Conseil canadien des normes (CCN) conformément aux exigences et lignes directrices du CCN. On trouvera des renseignements supplémentaires sur les Normes nationales du Canada à l'adresse : www.ccn.ca.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada (ISDE). Dans le but d'améliorer la compétitivité économique du Canada et le bien-être collectif de la population canadienne, l'organisme dirige et facilite l'élaboration et l'utilisation des normes nationales et internationales. Le CCN coordonne aussi la participation du Canada à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

En outre, il fournit des services d'accréditation à différents clients, parmi lesquels des organismes de certification de produits, des laboratoires d'essais et des organismes d'élaboration de normes. On trouvera la liste des programmes du CCN et des organismes titulaires de son accréditation à l'adresse : www.ccn.ca.

NORME NATIONALE DU CANADA

CAN/CGSB-72.34-2024

Remplace CAN/CGSB-72.34-2017
Confirmée, mars 2022

Enregistrements électroniques utilisés à titre de preuves documentaires

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN BOTH FRENCH AND ENGLISH.

ICS 37.080

Publiée en juin 2024 par
l'Office des normes générales du Canada
Ottawa (Ontario) K1A 0S5

Office des normes générales du Canada

Comité de gestion des documents et images électroniques

(Membres votants à la date de scrutin)

Présidente (non votante)

Luciana Duranti	InterPARES (Intérêt général)

Catégorie intérêt général

Corinne Rogers	InterPARES
Jake V. Knoppers	Expert-conseil
Lois M. Evans	Land Title and Survey Authority of British Columbia
Louise Spiteri	Université Dalhousie
Stuart Rennie	Expert-conseil en gestion de documents

Catégorie producteur

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

Catégorie organisme de réglementation

David Charles	Agence du revenu du Canada
Maryse Kiese	Agence des services frontaliers du Canada
Michael Mohammed	Secrétariat du Conseil du Trésor du Canada

Catégorie utilisateur

Heather Houston	Services publics et Approvisionnement Canada
Rebecka Sheffield	Association canadienne des archivistes
Robert Weisman	Université d’Ottawa
Sharon Smith	Bibliothèque et Archives Canada
Uta Fox	Service de police de Calgary

Gestionnaire du comité (non votant)

Robert Long	Office des normes générales du Canada

Nous remercions Corinne Rogers et Lois M. Evans d’avoir dirigé le groupe de travail lors de la révision de la dernière édition de la présente norme.

La traduction de la présente Norme nationale du Canada a été effectuée par le gouvernement du Canada.

Préface

La présente Norme nationale du Canada CAN/CGSB-72.34-2024 remplace l'édition de 2017, y compris le modificatif d'octobre 2018 et la confirmation de mars 2022.

Changements depuis la dernière édition

Par changement, on entend toute révision mineure du contenu de la norme visant à corriger des omissions, des erreurs de fait, des redondances au sein de la norme, les doubles emplois dans la norme en lien avec les pratiques exemplaires reconnues mentionnées dans d'autres normes, ou encore des modifications apportées aux fins de clarté et comme bases de connaissances. Les changements notables sont les suivants :

- Modification de la section 3, Termes et définitions, notamment suppression de termes non utilisés dans la norme, clarification de plusieurs termes et ajout de termes.

- Modification de la section 5, Exigences des lois régissant les enregistrements électroniques utilisés à titre de preuves documentaires, à des fins de clarté.

- Modification de la section 6, Programme de gestion des enregistrements. Des changements mineurs et considérables ont été apportés à des fins de clarté et pour faire ressortir l'information essentielle.

- Modification de la section 7, Gestion du système de la TI pour en faire une section distincte et renforcer les passages sur l'évaluation des risques et la protection des renseignements personnels. Aussi, ajout de l'article 7.4, Sécurité et protection.

- Suppression des annexes informatives et ajout des renseignements essentiels que ces annexes contenaient au corps de la norme.

- Examen et mise à jour des sources et références dans la bibliographie.

Les définitions suivantes s'appliquent lorsqu'il s'agit de comprendre comment mettre en œuvre une Norme nationale du Canada :

- « doit » indique une **exigence obligatoire**;

- « devrait » exprime une **recommandation**;

- « peut » exprime une **permission**, une **possibilité**, ou une **option**, par exemple, qu'un organisme peut faire quelque chose.

Les notes accompagnant les articles ne renferment aucune exigence ni recommandation. Elles servent à séparer du texte les explications ou les renseignements qui ne font pas proprement partie du corps de la norme. Les annexes sont désignées comme normative (obligatoire) ou informative (non obligatoire) pour en préciser l'application.

Table des matières

Page

Avant-propos

La norme CAN/CGSB-72.34 établit les principes, méthodes et pratiques de création (c'est-à-dire production, réception et saisie) et de gestion d'enregistrements électroniques de tous genres (p. ex., courriels, documents cartographiques ou audiovisuels, textes, fichiers multimédias, etc.) pour en favoriser l'admissibilité (admissibilité [d'un enregistrement], admissibilité [règles d'admissibilité] et poids [de la preuve]) en tant que preuves dans le cadre de procédures judiciaires. Comme l'information juridique, technique et en matière de gestion présentée dans cette norme est d'ordre général seulement, il est recommandé aux usagers d'obtenir des conseils d'experts avant d'appliquer les recommandations de la norme à des enregistrements ou à des systèmes particuliers.

La présente norme s'harmonise aux lois fédérales, provinciales et territoriales et à leurs règlements d'application qui étaient en vigueur au moment des délibérations du comité. Lorsqu'une loi ou un règlement et la présente norme ne concordent pas, c'est la loi ou le règlement qui a préséance.

Introduction

À propos de la présente norme

Une organisation peut être tenue de présenter des enregistrements électroniques à titre de preuves dans une procédure judiciaire. Pour favoriser l'admissibilité et le poids (ou la valeur probante) d'enregistrements électroniques utilisés à titre de preuves documentaires, l'organisation doit veiller à ce que la fiabilité, l'exactitude et l'authenticité, c'est-à-dire la légitimité, de ces enregistrements puissent être prouvées ou présumées. Pour assurer la crédibilité de ses enregistrements électroniques, une organisation devrait se conformer à la présente norme.

On utilise l'expression « enregistrement électronique » plutôt que l'expression « enregistrement numérique » dans la présente norme. En effet, les « enregistrements numériques » se composent de valeurs binaires discrètes réunies en une ou plusieurs chaînes de bits, tandis que les « enregistrements électroniques » comprennent les enregistrements numériques ainsi que les enregistrements analogues transmis par conducteurs électriques qui nécessitent de passer par un équipement électronique pour être lus par l'être humain.

La présente norme est neutre sur le plan de la technologie de l'information; en d'autres termes, elle ne tient pour acquis ni n'approuve aucun environnement de système, système de gestion de bases de données, paradigme de conception de bases de données, méthodologie d'élaboration de systèmes, langage de définition de données, langage de commande, interface système, interface utilisateur, syntaxe, plate-forme informatique ou technologie d'exploitation en particulier. La norme repose sur une approche intégrée et interopérable en matière de systèmes de gestion des enregistrements électroniques.

La norme présente un cadre et des lignes directrices pour la mise en œuvre et l'exploitation de systèmes d'enregistrements électroniques, que l'information qui s'y trouve soit ou non jamais requise à titre de preuve. Par conséquent, la conformité à la norme devrait être considérée comme une démonstration d'une gestion opérationnelle responsable. L'application de la norme aux activités d'une organisation n'éliminera pas la possibilité d'un litige, mais il est probable qu'elle facilitera la production d'enregistrements électroniques et rendra plus certaine leur acceptation dans le cadre de procédures judiciaires.

Relation avec les exigences des lois canadiennes sur la preuve

Les enregistrements enregistrés ou mis en mémoire au moyen d'une technologie électronique peuvent être admissibles en preuve dans une procédure judiciaire au Canada. Si leur admissibilité est mise en doute, les enregistrements devront satisfaire à certaines exigences en matière d'admissibilité des lois et, dans certains cas, de la common law. Ces exigences peuvent varier selon la fin à laquelle les enregistrements sont présentés en preuve. Comme la plupart des lois provinciales et territoriales sur la preuve, la *Loi sur la preuve au Canada* (LPC) renferme la disposition suivante qui encourage l'utilisation de normes :

« Afin de déterminer si, pour l'application de toute règle de droit, un document électronique est admissible, il peut être présenté un élément de preuve relatif à toute norme, toute procédure, tout usage ou toute pratique touchant la manière d'enregistrer ou de mettre en mémoire un document électronique, eu égard au type de commerce ou d'entreprise qui a utilisé, enregistré ou mis en mémoire le document électronique ainsi qu'à la nature et à l'objet du document. »

Utilisation de la présente norme dans le cadre d'une procédure judiciaire

Dans une procédure judiciaire, la présente norme pourrait éclairer la préparation d'arguments au sujet du sens à donner aux termes clés utilisés dans les règles d'admissibilité des enregistrements électroniques, soit « intégrité d'un système de la TI » et « intégrité de l'enregistrement », qu'on retrouve dans les dispositions des lois sur la preuve qui concernent les enregistrements électroniques, ainsi que l'expression les enregistrements produits « dans le cours usuel et ordinaire des affaires » telle qu'elle apparaît dans la LPC.

Termes et définitions

La présente norme utilise des termes et définitions inspirés de normes, lignes directrices et politiques nationales et internationales pertinentes.

Versions anglaise et française de la présente norme

Par souci de cohérence entre la version anglaise et la version française, les principes suivants ont été respectés. Lorsque la version anglaise utilise le terme « record », la version française utilise l'équivalent « enregistrement ». Chaque fois que la version anglaise utilise le terme « document », l'équivalent « document » est utilisé dans la version française.

Compte tenu de l'usage canadien, quelques termes utilisés dans la version française de la norme CAN/CGSB-72.34 diffèrent des termes utilisés en français international. Par exemple, les expressions « final disposition », « preservation », « record » et « records management » dans la version anglaise sont respectivement rendues par « élimination », « préservation », « enregistrement » et « gestion des enregistrements » dans la version française.

Enregistrements électroniques utilisés à titre de preuves documentaires

1 Objet

1.1 La présente Norme nationale du Canada fournit des consignes pour l'élaboration de politiques, de procédures, de processus et de documentation qui permettront de préserver la fiabilité, l'exactitude et l'authenticité des enregistrements électroniques afin de :

a) veiller à ce que les enregistrements électroniques puissent appuyer de manière fiable des décisions d'affaires et des échanges d'engagement;

b) appuyer l'admissibilité et la valeur probante des enregistrements électroniques dans des procédures judiciaires;

c) protéger la capacité des enregistrements électroniques de documenter effectivement les décisions, les actions et les transactions d'une organisation et de demander des comptes aux personnes qui en sont responsables.

1.2 La présente norme s'applique aux organisations qui produisent, reçoivent, saisissent, conservent, gèrent, utilisent, transmettent, éliminent ou mettent en mémoire de l'information sous forme électronique, ainsi qu'aux activités du secteur privé et du secteur public, qu'il s'agisse d'activités à but lucratif ou sans but lucratif.

1.3 La présente norme a pour but de veiller à ce que les enregistrements électroniques dans les systèmes d'enregistrements soient crédibles. Les usagers typiques comprennent :

a) les gestionnaires d'organisations du secteur privé et du secteur public;

b) les professionnels des systèmes de la TI et des systèmes de gestion des enregistrements;

c) les professionnels du droit et les personnes responsables des services de sécurité et de la gestion des risques;

d) les personnes responsables de la création (c'est-à-dire production ou réception ou mise en mémoire) et de la tenue à jour des enregistrements d'une organisation.

1.4 La présente norme expose des méthodes pour la gestion et la préservation d'enregistrements électroniques qui sont considérées comme des pratiques exemplaires, indépendamment de considérations d'ordre juridique. Par conséquent, les organisations qui se conforment à la présente norme en profiteront, même lorsqu'aucun enjeu judiciaire n'entre en ligne de compte.

1.5 De plus, la présente norme fournit des lignes directrices relatives à un cadre de procédures qui appuie des pratiques de qualité en matière de gestion des enregistrements et la définition et la mise en œuvre de mesures appropriées pour protéger la valeur probante des enregistrements électroniques, y compris leur intégration aux processus de conception et de gestion des enregistrements et des systèmes de la TI.

2 Références normatives

Les documents normatifs suivants renferment des dispositions qui, par renvoi au présent document, constituent des dispositions de la présente Norme nationale du Canada. Les documents de référence peuvent être obtenus auprès des sources mentionnées ci-après.

Note : Les coordonnées indiquées ci-dessous étaient valides à la date de publication de la présente norme.

Sauf indication contraire de l'autorité appliquant la présente norme, toute référence non datée s'entend de l'édition ou de la révision la plus récente de la référence ou du document en question. Une référence datée s'entend de la révision ou de l'édition précisée de la référence ou du document en question.

2.1 Ministère de la Justice

Loi sur la preuve au Canada (LPC)

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

2.1.1 Coordonnées

Les publications susmentionnées peuvent être obtenues auprès du ministère de la Justice Canada, Direction générale des communications, Division des affaires publiques. Téléphone : 613-957-4222. Site Web : http://canada.justice.gc.ca.

2.2 Les lois sur la preuve de chaque administration provinciale et territoriale peuvent être obtenues de leurs sites Web de la législation respectifs.

2.3 Les autres sources qui ont été considérées lors de l'élaboration de la présente norme sont énumérées dans l'annexe A.

3 Termes et définitions

Pour les besoins de la présente Norme nationale du Canada, les termes et définitions suivants s'appliquent.

accès
droit, possibilité ou moyen de trouver, de consulter ou d'extraire l'information enregistrée.

admissibilité (d'un enregistrement)
capacité de l'information enregistrée d'être produite en preuve dans une procédure judiciaire.

admissibilité (règles d'admissibilité)
règles en vertu desquelles les enregistrements sont jugés acceptables à titre de preuves dans une procédure judiciaire.

assurance de la qualité (des enregistrements)
procédures permettant de surveiller et d'évaluer le système d'enregistrement dont l'objet est de maintenir un niveau de qualité souhaité.

audit
examen systématique des activités permettant de veiller à ce que l'information enregistrée soit conforme aux politiques, aux procédures et aux contrôles établis et mis en œuvre de façon à ce que toutes les obligations financières, opérationnelles, juridiques et réglementaires soient satisfaites.

authenticité
qualité d'une entité qui est ce qu'elle est censée être et n'a pas été altérée ou corrompue.

authentification
déclaration de l'authenticité à un moment particulier.

chiffrement
conversion de l'information enregistrée en un code secret (ou d'un texte en clair en texte chiffré).

classification des enregistrements
organisation systématique des enregistrements en groupes ou en catégories selon diverses méthodes, procédures ou conventions représentées dans un plan ou un schéma.

communication de la preuve en format électronique (communication électronique)
procédure préalable au procès qui nécessite un échange d'enregistrements électroniques pertinents entre les parties.

contrôle de l'accès
processus qui consiste à n'accorder qu'aux seules personnes autorisées l'accès aux enregistrements dans le système d'enregistrements.

conversion
processus de transformation de l'information enregistrée d'un format à un autre.
Voir aussi *migration*.

copie
double de l'information enregistrée.

cycle de vie des enregistrements
modèle de gestion des enregistrements et science archivistique qui déterminent la durée de vie d'un enregistrement par ordre séquentiel : création (production, réception ou saisie); classification; tenue à jour et utilisation; évaluation; disposition par destruction ou transfert à une institution ou à un service d'archivage; préservation; description dans les moteurs de recherche archivistiques; référence et accès.

défaut de produire une preuve
destruction, falsification ou dissimulation de preuve.

destruction (des enregistrements)
processus qui consiste à éliminer des enregistrements de façon à ce qu'il soit impossible de les reconstituer.

disposition (des enregistrements)
mesure définitive prise au sujet des enregistrements après l'expiration de leur période de conservation prescrite.

document
unité indivisible d'information enregistrée qui présente un contenu stable et une forme fixe.

donnée
plus petite unité significative d'information enregistrée.

enregistrement
tout document produit ou reçu par une organisation dans le cadre de son activité et en raison de ladite activité, et qui est conservé pour suite à donner ou référence.

enregistrement analogue
enregistrement écrit sous forme continue sur du matériel physique comme du papier, un film et des supports audio et vidéo.
Voir aussi *enregistrement*.

enregistrement authentique
enregistrement qui est ce qu'il est censé être et n'a pas été altéré ou corrompu.

enregistrement crédible
enregistrement exact, fiable et authentique.
Voir aussi *exactitude*, *fiabilité* et *authenticité*.

enregistrement électronique
enregistrement analogue ou numérique accessible au moyen d'un équipement électronique.
Voir aussi *enregistrement* et *enregistrement analogue*.

enregistrement numérique
enregistrement constitué de valeurs binaires discrètes réunies en une ou plusieurs chaînes de bits auquel on peut accéder à partir d'un ordinateur.

enregistrement officiel
instance d'un enregistrement qui a valeur d'enregistrement original final, complet et faisant autorité.

enregistrement original
premier enregistrement complet susceptible d'atteindre le but pour lequel il est prévu (c'est-à-dire d'être efficace).

Note : Un enregistrement original présente trois caractéristiques : l'antériorité (c'est-à-dire que l'enregistrement a été le premier à être généré, l'exhaustivité et l'efficacité.

enregistrement source (numérisation)
enregistrement analogue à partir duquel une copie électronique (numérique) est faite.
Voir aussi *enregistrement analogue.*

enregistrement temporaire
enregistrement qui n'a pas besoin d'être conservé pour répondre à des exigences et qui n'a pas de valeur permanente quant à la documentation ou à l'appui des activités de l'organisation.

évaluation des risques
évaluation de la probabilité qu'un événement négatif se produise et de la portée de ses conséquences, pour qu'on puisse s'y préparer.

exactitude
mesure dans laquelle l'information enregistrée est précise, conforme, vraie, libre d'erreur ou de distorsion.

fiabilité
qualité d'un enregistrement dont on peut compter que le contenu constitue une représentation complète et exacte des transactions, des activités ou des faits dont il atteste.

fiabilité d'un système de la TI
qualité d'un système qui a été testé, soumis à un examen par les pairs ou à une publication, qui est accepté au sein de la collectivité scientifique compétente et dont le taux d'erreur connu ou potentiel est acceptable.

format
moyen de coder des données de façon à ce qu'elles renferment de l'information au sujet de leur structure, de leur organisation et de leur contenu qui permettra qu'elles soient interprétées pour utilisation future dans le cadre d'activités de mise en mémoire, d'extraction, de traitement, de présentation, de manipulation et de transmission.

gestion des enregistrements
domaine de gestion qui concerne la création (production, réception ou saisie), la tenue à jour, l'utilisation et la disposition des enregistrements.

identité de l'enregistrement
totalité des attributs d'un enregistrement qui, ensemble, permettent d'en déterminer l'unicité et de le distinguer de tout autre enregistrement.

Note : Une composante de l'authenticité, comme l'intégrité de l'enregistrement.

information
message destiné à des fins de communication.

information enregistrée
information mise en mémoire sur un support de manière stable.

informatique en nuage
modèle qui offre un accès réseau omniprésent, pratique et sur demande à un groupe commun de ressources informatiques configurables qui peuvent être acquises rapidement et offertes selon un effort de gestion minime ou une interaction minime de la part du fournisseur du service.

intégrité d'un système de la TI
capacité démontrée d'un système de la TI d'exécuter ses fonctions prévues sans entrave, libre de toute manipulation non autorisée, qu'elle soit intentionnelle ou accidentelle, et l'existence de cette capacité au moment où l'information enregistrée a été générée et utilisée.

intégrité de l'enregistrement
qualité d'un enregistrement qui est complet et qui n'a été altéré dans aucun de ses aspects essentiels.

Note : Une composante de l'authenticité, comme l'identité de l'enregistrement.

intelligence artificielle
toute technologie de l'information qui exécute des tâches pour lesquelles il faut habituellement faire appel à l'intelligence biologique, comme comprendre le langage parlé, apprendre des comportements ou résoudre des problèmes.

manuel de gestion des enregistrements
document qui définit la portée du programme de gestion des enregistrements, ses pouvoirs et les services qu'il dispense ainsi que les concepts fondamentaux de la gestion des enregistrements.

métadonnées
données servant à définir un enregistrement et à en décrire l'utilisation, la gestion, l'historique de conservation et les changements technologiques.

migration
processus qui consiste à transférer de l'information enregistrée d'une configuration de système de TI à une autre. Voir aussi *conversion*.

mise en suspens pour des raisons juridiques
processus par lequel une organisation préserve toutes formes d'enregistrements susceptibles de se révéler pertinents lorsqu'une poursuite peut raisonnablement être anticipée ou est en cours.

numérisation
processus qui consiste à transposer sur un support numérique une information enregistrée sur un support analogue. Voir aussi *enregistrement analogue*.

obligation redditionnelle
principe selon lequel les personnes et les organisations, étant responsables de leurs actions, peuvent être appelées à rendre des comptes à leur sujet.

organisation
entité susceptible d'avoir des droits et des obligations prévus par la loi.

ouï-dire
déclaration faite à l'extérieur du tribunal par une personne autre que la personne en train de témoigner et qui est soumise pour faire foi de la véracité des faits déclarés.

panne du système de la TI
problème, défaut, défaillance ou catastrophe technique dans le fonctionnement d'un système de la TI.

période de conservation des enregistrements
période donnée pendant laquelle les enregistrements sont conservés pour répondre à des exigences opérationnelles, juridiques, réglementaires, financières ou autres.

personne autorisée
personne à qui une responsabilité précise a été confiée par une autorité qui a le pouvoir de le faire.

piste de vérification
registre des activités conservé dans le système de la TI qui permet la reconstitution, l'étude et l'examen de la séquence des activités se rapportant à une opération, une procédure ou un événement lors d'une transaction.

poids (de la preuve)
crédibilité ou valeur probante d'une preuve.

préservation (des enregistrements)
totalité des principes, politiques et stratégies qui permettent de contrôler les activités conçues pour assurer la stabilité physique et technologique de l'enregistrement et la protection du contenu intellectuel dans le temps.

preuve
tout moyen par lequel un fait allégué, dont la véracité est soumise à une investigation, est confirmé ou infirmé lors d'une procédure judiciaire.

preuve documentaire
information enregistrée admise en preuve dans une procédure judiciaire.

procédure
ensemble de règles, écrites ou non, qui régissent la conduite d'une transaction, ou les étapes formelles à franchir pour réaliser une transaction.

processus
série de mesures ou d'événements qui se déroulent de façon définie menant à l'accomplissement d'un résultat attendu.

programme de gestion des enregistrements
programme conçu pour appuyer la création, la gestion, l'utilisation, la disposition et la préservation des enregistrements crédibles.

saisie
action d'enregistrer ou de sauvegarder une instance en particulier d'une information enregistrée.

sauvegarde (copie)
copie exacte des systèmes électroniques, des programmes, des données et des renseignements actifs faite à des fins de reprise ou de récupération en cas de panne du système.

sécurité de l'information
discipline multidimensionnel dont l'objet est de protéger l'information enregistrée, sans égard au lieu, contre toute menace, et ce, par une combinaison de moyens (techniques, organisationnels, humains et juridiques).

signature électronique sécurisée
signature électronique qui résulte de l'application de toute technologie ou de tout procédé prévu par le *Règlement sur les signatures électroniques sécurisées* (DORS/2005-30) pris en vertu du paragraphe 48(1) de la LPRPDE.

support
dispositif matériel sur lequel l'information enregistrée est mise en mémoire.

système d'enregistrements
système informatique avec lequel ou dans lequel l'information est enregistrée ou mise en mémoire, y compris toute procédure connexe.

système de TI
ensemble composé d'un ou de plusieurs ordinateurs, des logiciels connexes, périphériques et terminaux, des interventions humaines, processus matériels et moyens de transfert de l'information s'y rapportant qui constitue un tout autonome susceptible d'assurer le traitement et/ou le transfert de l'information.

système décisionnel automatisé
comprend toute technologie qui soit informe soit remplace le jugement des décideurs humains. Ces systèmes proviennent de domaines tels que les statistiques, la linguistique et les sciences informatiques, et utilisent des techniques telles que les systèmes basés sur des règles, la régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage en profondeur et les réseaux neuronaux.

tenue des enregistrements
saisie, mise en mémoire, utilisation, tenue à jour et disposition des enregistrements et de leurs métadonnées.

valeur probante
poids ou crédibilité accordée à une preuve.
Voir aussi *poids*.

4 Acronymes, sigles et abréviations

Les sigles et abréviations suivants sont utilisés dans la présente norme :

AE	Agent préposé aux enregistrements
EAT	Examen assisté par la technologie
GE	Gestion des enregistrements
LCP	*Loi sur la preuve au Canada*
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
TI	Technologie de l'information

5 Exigences des lois régissant les enregistrements électroniques utilisés à titre de preuves documentaires

5.1 Généralités

Le principe premier avancé par la présente norme est qu'une organisation doit toujours être en mesure de produire ses enregistrements en preuve. L'organisation doit, en tout temps, assurer le contrôle de l'information enregistrée, y compris lorsqu'une politique de télétravail est en place.

La conformité systématique à la présente norme est un élément essentiel pour prouver l'intégrité d'un enregistrement électronique ou d'un système d'enregistrements. Une conformité occasionnelle peut être préférable à l'absence de conformité, mais elle ne suffit pas à prouver l'intégrité. Par conséquent, il n'est pas suffisant de se conformer uniquement lorsque des procédures judiciaires sont prévues ou engagées.

Les articles de la *Loi sur la preuve au Canada* (LPC) mentionnés ci-dessous ne s'appliquent qu'aux procédures judiciaires assujetties aux lois fédérales :

a) les documents originaux sur papier admissibles à titre d'enregistrements commerciaux en vertu de dispositions comme celles de l'article 30 de la LPC;

b) les enregistrements électroniques admissibles en vertu de dispositions comme celles de l'article 31 de la LPC;

c) les enregistrements microfilmés, numérisés ou saisis à titre d'images admissibles en vertu de dispositions sur la copie comme celles de l'article 30 de la LPC ou de dispositions sur les enregistrements électroniques comme celles de l'article 31 de la LPC;

d) les sorties imprimées utilisées comme document relatant l'information contenue dans un enregistrement électronique admissibles en vertu de dispositions comme celles de l'article 31.2(2) de la LPC;

e) les enregistrements créés au moyen d'un échange de données informatisé (EDI) admissibles en vertu de dispositions comme celles de l'article 31 de la LPC.

On trouve des dispositions comparables dans les lois des provinces et territoires qui s'appliquent aux procédures judiciaires assujetties aux lois de ces administrations.

Comme les lois et les normes régissant l'admissibilité en preuve des enregistrements électroniques et des documents sur papier diffèrent, la gestion de ces enregistrements peut aussi différer. Les lois de la preuve s'appliquant aux procédures judiciaires des régimes fédéraux, provinciaux et territoriaux permettent le remplacement de documents sources imprimés, ou de leurs copies, par des documents, y compris des images, électroniques (ou des enregistrements). Pour être admissible, une pièce produite électroniquement, peu importe sa nature, doit se conformer aux dispositions régissant les enregistrements (ou pièces) électroniques des lois des administrations en cause.

5.2 Exigences régissant l'admissibilité des enregistrements électroniques utilisés à titre de preuves documentaires

Pour utiliser un enregistrement électronique à titre de preuve, il faut prouver l'authenticité de l'enregistrement, qui peut être déduite de l'intégrité du système d'enregistrements électroniques dans lequel l'enregistrement est produit ou reçu ou mis en mémoire et de la preuve que l'enregistrement a été produit « dans le cours usuel et ordinaire des affaires » ou qu'il n'est pas assujetti à la règle juridique interdisant le ouï-dire (voir l'article 30 de la LPC par exemple).

5.2.1 Authenticité de l'enregistrement

Un enregistrement soumis en preuve doit être authentifié en présentant une preuve externe à l'enregistrement lui-même (p. ex. le témoignage d'un témoin de la création de l'enregistrement) démontrant qu'il est bien ce qu'il est censé être (que son identité et son intégrité sont intactes), voir l'article 31.1 de la LPC. Il s'agit de la règle d'authentification. Ou encore, un enregistrement peut être déclaré authentique si l'intégrité du système d'enregistrements dans lequel l'enregistrement a été produit ou reçu ou mis en mémoire et/ou la fiabilité des processus de tenue des enregistrements utilisés peuvent être démontrées.

5.2.2 Intégrité du système d'enregistrements électroniques

Si une partie fournit un enregistrement comme preuve de la véracité de son contenu, la règle de la meilleure preuve s'applique. Selon la règle de la meilleure preuve, l'original d'une pièce (ou preuve primaire) est préféré à toute copie (ou preuve secondaire). Dans les cas où il y a plus d'une instance d'un même enregistrement, l'organisation doit déterminer quelle instance constitue l'enregistrement officiel de l'organisation (preuve primaire).

Si la partie qui fournit une preuve secondaire peut expliquer de manière satisfaisante l'absence de preuve primaire de façon à réfuter toute allégation de fraude, la preuve secondaire sera alors admissible. En ce qui concerne les enregistrements électroniques, l'application de la règle de la meilleure preuve pose problème à cause de l'absence, dans l'environnement numérique, des éléments traditionnellement considérés comme des originaux. Par conséquent, la législation sur la preuve stipule que la règle de la meilleure preuve peut être satisfaite par une preuve de l'intégrité du système d'enregistrements, conformément à l'alinéa 31.2(1)(a) de la LPC.

Cette « intégrité » peut être confirmée, sauf preuve contraire, par une preuve démontrant :

a) que le système d'enregistrements électroniques fonctionnait correctement à l'époque en cause, ou, dans le cas contraire, que son mauvais fonctionnement n'a pas compromis l'intégrité de l'enregistrement électronique, et qu'il n'existe aucun autre motif raisonnable de mettre en doute l'intégrité du système (p. ex. paragr. 31.3(a) de la LPC);

b) que l'enregistrement électronique présenté en preuve par une partie a été enregistré ou mis en mémoire par une partie adverse (p. ex. 31.3(b) de la LPC);

c) que l'enregistrement électronique a été enregistré ou mis en mémoire « dans le cours usuel et ordinaire des affaires » par une personne qui n'est pas partie à la poursuite et qui ne relevait pas de l'autorité de la partie qui cherche à le présenter en preuve (p. ex., paragraphe 31.3(c) de la LPC).

5.2.3 Pièce établie « dans le cours usuel et ordinaire des affaires »

Si une partie présente un enregistrement comme preuve de la véracité du contenu, la règle du ouï-dire s'applique également (voir ouï-dire). Il y a une exception à la règle du ouï-dire pour les enregistrements commerciaux, car la présomption est que les organisations appliqueraient des procédures d'enregistrement assurant la fiabilité de l'information enregistrée. Une exception à la règle du ouï-dire s'applique aux enregistrements commerciaux s'il est prouvé qu'ils ont été « établis dans le cours usuel et ordinaire des affaires » de l'organisation dont provient l'enregistrement (p. ex. l'art. 30 de la LPC). La définition du terme « affaires » est vaste : « tout commerce ou métier ou toute affaire, profession, industrie ou entreprise de quelque nature que ce soit exploités ou exercés au Canada ou à l'étranger […] » (paragr. 30(12) de la LPC).

Comme c'est le cas pour la règle d'authentification et la règle de la meilleure preuve, l'exception à la règle du ouï-dire peut être appliquée aux enregistrements commerciaux s'il y a preuve de l'intégrité du système d'enregistrements dans lequel les enregistrements présentés en preuve ont été produits ou reçus ou mis en mémoire.

5.2.4 Preuve de l'intégrité du système d'enregistrements d'une organisation

Les éléments suivants peuvent être invoqués pour prouver l'intégrité du système d'enregistrements électroniques d'une organisation :

a) sources : l'origine des données figurant dans les enregistrements du système électronique est connue;

b) contemporanéité : les enregistrements électroniques ont été produits ou reçus ou mis en mémoire dans un délai raisonnable suivant les événements auxquels ils se rapportent ou mis en mémoire dans un délai raisonnable suivant leur réception;

c) données commerciales courantes : les données contenues dans un enregistrement correspondent à un genre de données régulièrement transmises à l'organisation d'origine ou ont été créées par elle à l'occasion de ses activités régulières;

d) entrée des données : les procédures d'entrée des données s'inscrivent dans le cours usuel et ordinaire des affaires de l'organisation et sont mises en œuvre conformément au manuel de gestion des enregistrements (manuel de GE) et au guide de gestion du système de la TI (voir 6.4 et 6.5);

e) normes : l'organisation se conforme aux normes applicables sur la gestion des enregistrements électroniques selon 6.3.2 b);

f) prise de décisions : les décisions prises par l'organisation se fondent sur les enregistrements électroniques contenus dans son système d'enregistrements électroniques;

g) logiciels : les logiciels de l'organisation permettent d'exploiter de manière fiable son système d'enregistrements électroniques et d'assurer le traitement de ses données;

h) changements apportés dans le système : un registre des changements et modifications dans le système est tenu;

i) protection des renseignements personnels : l'utilisation qui est faite des données dans les enregistrements électroniques de l'organisation est conforme aux lois canadiennes, provinciales et territoriales pertinentes sur le respect de la vie privée régissant la collecte, l'utilisation ou la divulgation de renseignements personnels, confidentiels ou commerciaux, de secrets commerciaux ou d'autres renseignements privilégiés ou confidentiels;

j) sécurité : des procédures de sécurité, par exemple des mesures de protection contre l'accès sans autorisation et des plans de reprise après sinistre, sont utilisées pour garantir l'intégrité du système d'enregistrements électroniques.

La preuve de l'existence de ces éléments est fournie dans le manuel de gestion des enregistrements (voir 6.4) et dans le guide de gestion du système de la TI (voir la section 7).

5.3 Communication de la preuve en format électronique (communication électronique) et préparatifs en vue d'une poursuite

La communication de la preuve en format électronique est une procédure qui se déroule avant le procès dans une poursuite civile dans le cadre de laquelle les parties échangent des enregistrements électroniques pertinents, qui peuvent notamment comprendre des métadonnées. Les investigations et les enquêtes comportent aussi la collecte et la production d'enregistrements électroniques, parfois très nombreux. Il existe un système parallèle à découverte du droit civil aux fins de divulgation dans les procédures du droit pénal comprenant les demandes préalables aux procès, les demandes de renseignements préliminaires et les audiences voir-dire tenues pendant un procès. Les énormes volumes, les formats variés et la volatilité des enregistrements électroniques présentent de nombreux défis.

Le premier défi consiste à identifier des sources possibles d'information pertinente. Les organisations qui disposent d'un système d'enregistrements électroniques bien géré seront en mesure de trouver, de préserver et de recueillir des enregistrements pertinents beaucoup plus rapidement, plus précisément et plus économiquement que les organisations dont les enregistrements électroniques sont désorganisés. Par conséquent, une organisation devrait avoir en place un système de gestion des enregistrements électroniques bien avant que la nécessité de communiquer une preuve électronique se présente. Un deuxième défi des points de vue du temps et du coût est celui de l'examen des enregistrements et le traitement des documents, lequel est de plus en plus effectué par des systèmes informatiques automatisés. La communication électronique nécessite davantage l'examen de milliers d'enregistrements pour en déterminer la pertinence et le caractère confidentiel. Ce genre d'examen, beaucoup plus fréquent, se fait à l'aide d'outils d'apprentissage automatique (examen assisté par la technologie ou EAT, voir 5.3.1). Les organisations qui sont en mesure de recueillir efficacement seulement les enregistrements

pertinents (par exemple selon le type d'enregistrement, la date de l'enregistrement, l'auteur, le destinataire ou l'objet) feront des économies au moment de l'examen. Un troisième défi pour les organisations est la nécessité de produire les enregistrements électroniques pertinents exigés par le tribunal afin que ces enregistrements puissent être admissibles à titre de preuve dans les procédures judiciaires. Pour de plus amples renseignements sur la communication électronique de la preuve dans les litiges civils, se reporter aux principes de Sedona Canada (voir la note de bas de page 1). En ce qui concerne la communication de la preuve dans les procédures de droit pénal, voir R. v. Oler (D.M.) et al., 2014 ABPC 130 (CanLII).

5.3.1 Examen assisté par la technologie et d'autres outils et techniques automatisés

L'organisation pourra demander à son équipe juridique et à l'agent préposé aux enregistrements (AE) de faire un examen assisté par la technologie (EAT) pour satisfaire aux exigences de la communication électronique. Les modèles d'EAT sont nombreux et peuvent comprendre des modèles de recherche probabiliste reposant sur les interrelations entre les mots, la proximité et la fréquence; des modèles de recherche vague reposant sur les composantes de base de chaque mot de façon à en saisir toutes les formes possibles; des modèles de recherche par grappes, reposant sur un examen de groupes de documents ayant un contenu semblable; et des modèles de catégorisation de la recherche, qui font appel à un thésaurus. Les applications d'EAT sont tout aussi variées, allant des systèmes de catégorisation automatique à des systèmes d'analyse virtuelle en passant par les systèmes d'élimination des doublons, de chaînage des courriels et de codage prédictif.

Toutefois, les tribunaux ne seront peut-être pas toujours du même avis au sujet de la précision de ces dispositifs. Pour obtenir des renseignements sur la façon de mener une communication électronique à l'aide d'un EAT, voir les *principes de Sedona Canada.*

5.4 Mise en suspens pour des raisons juridiques

Une mise en suspens pour des raisons juridiques correspond à l'obligation de préserver l'information enregistrée et s'applique dès qu'une poursuite est envisagée ou qu'une partie menace de l'intenter[1]. Toutefois, la détermination du moment où ce point est atteint nécessite les conseils d'un juriste. Il peut être difficile de le déterminer aux premiers stades d'un différend. Des mesures de mise en suspens décidées trop tôt peuvent entraîner des coûts et des efforts disproportionnés. Mais si la mise en suspens des procédures normales de disposition est retardée, des preuves peuvent être perdues et des pénalités imposées pour défaut de produire une ou des preuves. Par conséquent, une évaluation de la bonne foi reposant sur des conseils juridiques devrait être faite.

Un avis concernant la nécessité d'imposer une mise en suspens pour des raisons juridiques en vue de préserver les documents en format papier et en format électronique doit être transmis à toutes les parties touchées, y compris les intervenants autres que les parties qui jouent un rôle pertinent et le personnel TI et de gestion des enregistrements de l'organisation. Cet avis doit donner des instructions claires et détaillées sur les genres d'information à préserver. Les gardiens des enregistrements doivent être informés du moment où ces exigences en matière de préservation sont levées.

Le système d'enregistrements doit pouvoir suspendre la disposition des enregistrements (et de toute autre information enregistrée) assujettis à une mise en suspens pour des raisons juridiques, un audit, un examen, une investigation, une enquête, une demande d'accès à l'information ou d'autres procédures juridiques ou administratives. L'AE, en consultation avec le conseiller juridique, la TI et les gestionnaires opérationnels, doit produire par écrit et mettre en application une procédure de mise en suspens pour des raisons juridiques qui définira notamment les éléments suivants :

---

[1] Les principes de Sedona Canada est le titre d'un projet du groupe de travail 7 de la conférence de Sedona (Sedona Canada). La « Conférence Sedona » tire son nom de Sedona, en Arizona, où elle a son siège social. On peut télécharger un exemplaire en PDF de ces principes à partir du site Les principes de Sedona Canada à https://thesedonaconference.org/node/9995. Selon le principe 3 des Principes de Sedona Canada, « Dès qu'il est raisonnable d'anticiper une poursuite, les parties devraient immédiatement envisager leur obligation de prendre de bonne foi des mesures raisonnables afin de préserver les documents électroniques potentiellement pertinents. »

a) la personne ou le poste au sein de l'organisation qui est autorisé à émettre, modifier ou abroger une mise en suspens pour des raisons juridiques;

b) le processus de coordination avec les conseillers juridiques de l'organisation;

c) le processus qui servira à gérer la mise en suspens pour des raisons juridiques et à veiller à ce que la mise en suspens soit respectée;

d) le processus par lequel les gardiens et les sources de données seront désignés adéquatement;

e) les systèmes de la TI essentiels pour la mise en suspens pour des raisons juridiques;

f) la protection des enregistrements contre tout accès non autorisé et contre toute modification;

g) les mesures prises pour documenter le processus de mise en suspens pour des raisons juridiques.

La procédure doit prévoir la formation du personnel sur la façon de mettre en œuvre et de gérer la mise en suspens pour des raisons juridiques et de l'administrer sans s'exposer à des sanctions pour dissimulation de preuve. La procédure doit indiquer que les tribunaux disposent de diverses options pour sanctionner une partie qui falsifie des preuves pertinentes, et notamment les sanctions suivantes :

a) ordonner la conservation, la garde ou la préservation de la preuve;

b) tirer une conclusion défavorable à l'encontre de la partie coupable du défaut de produire la preuve;

c) refuser d'admettre la preuve;

d) refuser d'entendre des témoins;

e) refuser d'autoriser une partie à interroger ou à contre-interroger un témoin;

f) imposer des frais judiciaires à la partie coupable du défaut de produire la preuve;

g) rendre une ordonnance d'outrage au tribunal à l'encontre de la partie coupable du défaut de produire la preuve;

h) rendre un jugement par défaut ou prononcer un non-lieu (décision judiciaire).

S'il est à craindre qu'une preuve pertinente ne soit pas conservée, le tribunal peut ordonner qu'une partie aux procédures judiciaires soit autorisée à faire des copies ou à prendre possession de la preuve entre les mains d'une autre partie.[2]

Pour ces raisons, la mise en suspens pour des raisons juridiques relève potentiellement de chaque personne au sein de l'organisation.

[2] Une telle ordonnance d'un tribunal est dite « ordonnance Anton Piller ». Elle est utilisée par exemple lorsqu'il est essentiel que le plaignant puisse inspecter la preuve afin que justice puisse être rendue si le risque est grand que des éléments de preuve essentiels soient détruits. La Cour suprême du Canada a fourni des éclaircissements sur les conditions nécessaires au prononcé et à l'exécution adéquate d'une ordonnance Anton Piller dans l'arrêt https://decisions.scc-csc.ca/scc-csc/scc-csc/fr/item/2309/index.do, [2006] 2 RCS 189, 2006 CSC 36.

5.5 Signatures

5.5.1 Signature électronique

Les dispositions de la LPC et de la LPRPDE régissent l'utilisation des signatures électroniques dans la loi fédérale. On retrouve des dispositions similaires dans les lois des provinces et des territoires portant sur les signatures électroniques. La fonction de la signature, qui consiste à établir un lien entre une personne et un document, reste la même, qu'il s'agisse d'une signature apposée sur un document en format papier ou d'une signature associée à un document électronique. L'exigence d'une signature par une personne est satisfaite si la méthode utilisée permet d'identifier la personne de façon unique et témoigne de l'approbation de l'enregistrement électronique par cette personne, et si la méthode utilisée est fiable et appropriée dans toutes les circonstances et remporte l'assentiment des parties. Il est généralement convenu que « l'approbation » signifie seulement le consentement à faire sien un texte, de sorte que la signature n'est pas nécessairement limitée à celle qui est apposée pour avaliser un contrat. Par conséquent, une « signature électronique » peut se définir comme l'information électronique qu'une personne crée ou adopte afin de signer un document et qui figure dans le document, y est jointe ou lui est associée.

En vertu de la LPRPDE, une signature électronique (signature numérique) sécurisée renvoie à une signature électronique qui résulte de l'application de toute technologie ou de tout procédé pouvant établir ce qui suit :

a) la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à la personne;

b) l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de la personne au document électronique se fait sous la seule responsabilité de cette dernière;

c) la technologie ou le procédé peut être utilisé pour identifier la personne qui utilise la technologie ou le procédé;

d) la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.[3]

5.5.2 Signature manuscrite

Quand la conservation d'enregistrements portant une signature manuscrite (c'est-à-dire une signature apposée sur un document physique par un moyen physique) est exigée comme preuve d'approbation, d'autorisation, d'accusé de réception, de confirmation, de notarisation ou d'attestation d'un acte, cette exigence peut être satisfaite par la numérisation de l'enregistrement et la conservation de son image numérique, sous réserve que toutes les autres conditions régissant la numérisation des documents papier soient respectées. Comme l'information juridique, administrative et technique présentée dans la présente norme est d'ordre général, il est recommandé aux usagers d'obtenir des conseils d'experts avant d'en appliquer les recommandations à un enregistrement ou à un système de la TI en particulier.

5.6 Copies papier authentifiées aux fins de procédures judiciaires

Lorsque des copies papier d'enregistrements électroniques ont besoin d'être produites, elles devront être authentifiées comme étant des copies conformes des enregistrements électroniques pour appuyer leur admissibilité et leur poids en preuve dans une procédure judiciaire. La procédure de production et d'authentification des copies papier doit être documentée.

La procédure de production de la copie papier d'un enregistrement électronique stipule que la signature d'une personne autorisée doit être apposée afin d'authentifier la copie papier et pour en prouver l'authenticité en cas de besoin. Lorsque la copie papier diffère de l'enregistrement électronique dans sa structure, dans sa forme ou dans son contenu, la nature des différences, leurs causes et la façon dont elles se sont produites doivent être documentées dans le document d'authentification (p. ex., un affidavit).

---

[3] Voir le paragr. 48(2) de la LPRPDE et son *Règlement sur les signatures électroniques sécurisées* (DORS/2005-30). Voir aussi l'art. 31.8 de la LPC.

6 Programme de gestion des enregistrements

6.1 Généralités

Le programme de gestion des enregistrements (GE) est conçu pour appuyer la création, la gestion, l'utilisation, la disposition et la préservation des enregistrements crédibles. Les concepts, principes, méthodes et pratiques de gestion des enregistrements adoptés par l'organisation démontreront qu'un programme approprié de GE est en place et qu'il est intégré dans le cours usuel et ordinaire des affaires de l'organisation.

Le programme de GE doit appuyer un système d'enregistrements réunissant des procédures et contrôles d'enregistrement appropriés qui viennent compléter les procédures opérationnelles d'affaires. L'organisation doit :

a) mettre sur pied un programme de GE;

b) élaborer une politique de GE accompagnée de définitions et d'attribution des responsabilités;

c) concevoir des procédures de GE et rédiger la documentation connexe;

d) choisir et mettre en œuvre des technologies à l'appui du système d'enregistrements;

e) établir des mesures de protection des enregistrements, y compris des pistes de vérification et des copies de sauvegarde;

f) mettre sur pied un processus d'assurance de la qualité des enregistrements.

6.2 Mise sur pied du programme de GE

6.2.1 Autorisation

L'organisation doit autoriser, au moyen d'un instrument formel (p. ex., politique, directive, décret, règlement), la mise sur pied d'un programme de GE, y compris la création d'un manuel décrivant en détail son système d'enregistrements et exposant les politiques, rôles et responsabilités et les procédures relatives à la création, à la conservation et à la disposition des enregistrements. Le document d'autorisation doit renvoyer aux pouvoirs et responsabilités confiés à l'organisation par la loi en ce qui concerne le programme de GE; confirmer que le programme de GE est intégré dans le cours usuel et ordinaire des affaires de l'organisation; et indiquera que le programme de GE assure un contrôle intégré des enregistrements électroniques et des documents papier. En plus de désigner une personne ou le titulaire d'un poste comme étant le signataire autorisé (c'est-à-dire l'AE), le document d'autorisation doit définir les éléments suivants :

a) le pouvoir et la responsabilité de l'organisation de créer un programme de GE en vertu de la loi;

b) l'objet du programme de GE;

c) la portée du programme de GE (c'est-à-dire propriété, garde, contrôle et applicabilité) et toute exclusion;

d) la façon dont le programme de GE est mis en œuvre (c'est-à-dire désignation des responsabilités);

e) les procédures requises pour la GE (c'est-à-dire création des enregistrements, gestion, utilisation, destruction, transfert ou préservation);

f) l'assurance de la qualité requise certifiant que toutes les fonctions de GE sont remplies adéquatement;

g) l'autorisation d'effectuer des changements ou des révisions à son programme de GE.

6.2.2 Responsabilité

Le rôle de l'AE en tant que responsable de la mise en œuvre du programme de GE dans le cours usuel et ordinaire des affaires de l'organisation doit être clairement défini dans l'instrument formel d'autorisation de l'organisation (p. ex., politique, directive). L'organisation doit indiquer toute autre responsabilité confiée à l'AE et à d'autres personnes ou aux titulaires d'autres postes pour veiller au respect du programme de GE (p. ex., un agent de sécurité [AS] du système de la TI responsable d'assurer l'intégrité du système de la TI.)

6.2.2.1 Délégation de responsabilité

Une organisation peut mettre en œuvre un programme de GE ou déléguer la totalité ou une partie du programme à un tiers autorisé (p ex., un fournisseur de services externe). Si une partie ou la totalité du programme est délégué, les rôles et responsabilités du tiers autorisé doivent être clairement précisés et documentés, afin que la crédibilité des enregistrements électroniques ne soit pas compromise.

6.2.2.2 Fournisseurs de services externes

Le gouvernement du Canada n'interdit pas aux institutions gouvernementales au sens de la *Loi sur la protection des renseignements personnels* ou aux organisations au sens de la *Loi sur la protection des renseignements personnels et les documents électroniques* d'avoir recours à un fournisseur de services externe qui stocke des renseignements personnels à l'extérieur du Canada. Au Canada, certaines provinces exigent que les organismes publics s'assurent que les renseignements personnels dont ils assurent la garde et la surveillance soient stockés et accessibles seulement au Canada, sous réserve des exceptions législatives. Par conséquent, les organismes doivent consulter des juristes compétents ou d'autres professionnels pour assurer la conformité aux lois applicables.

Quand une organisation a recours à un fournisseur de services externe pour la totalité ou une partie de son programme de GE, le fournisseur de services externe doit se conformer aux exigences juridiques et réglementaires applicables des administrations pertinentes ainsi qu'à la politique et aux procédures de GE de l'organisation. Ces dispositions doivent être indiquées dans tout document contractuel ou norme de service.

6.2.2.3 Recours à un fournisseur de services externe

Dans le contrat conclu avec le fournisseur de services, la description détaillée des procédures, des processus et des pratiques doit englober tous genres de services, y compris la gestion des installations, le stockage, la conversion et la migration des enregistrements électroniques ainsi que la sécurité. L'objet du contrat est de veiller à ce que le fournisseur de services externe se conforme à la politique, aux procédures, aux processus et aux pratiques de l'organisation. L'organisation doit conserver une copie de la preuve de conformité du fournisseur de services externe et de l'efficacité et de la sécurité des services, ou doit avoir accès à une telle preuve.

L'organisation doit s'assurer que le fournisseur de services externe signe une entente de confidentialité et de protection des renseignements personnels ou qu'il soit tenu par contrat de protéger l'organisation contre toute violation de la confidentialité ou atteinte à la vie privée. Les organisations doivent veiller à ce qu'il soit indiqué dans leur entente contractuelle avec le fournisseur de services qu'elles doivent être informées immédiatement de toute violation de l'accès. L'entente doit également inclure des dispositions sur l'interruption de l'accès pour les ex-employés ou les employés suspendus.

L'entente doit stipuler que les exigences en matière de conservation et de disposition de l'organisation seront respectées et que les procédures connexes seront mises en application, et que les enregistrements sont protégés, préservés et détruits selon les directives. L'entente avec le fournisseur doit également stipuler que lorsqu'une poursuite, un audit ou une investigation gouvernementale a lieu ou est prévu, les activités de destruction planifiée seront immédiatement suspendues et que la période de conservation recommencera à courir seulement lorsque la mise en suspens n'est plus nécessaire.

6.3 Politique de gestion des enregistrements

6.3.1 Obligation d'avoir une politique de gestion des enregistrements

Une organisation doit avoir un instrument formel (ci-après appelé « politique de GE ») stipulant que la gestion des enregistrements électroniques fait partie intégrante du cours usuel et ordinaire des affaires.

Dans certains milieux, il est utile de combiner l'autorisation du programme de GE et la politique de GE en un seul instrument formel.

6.3.2 Contenu de la politique de gestion des enregistrements

La politique de GE doit renfermer les dispositions suivantes :

a) définir les enregistrements et le système d'enregistrements visés par l'instrument formel (c'est-à-dire politique ou règlement) ainsi que toute exclusion;

b) définir les normes pertinentes à la GE, aux affaires et à la TI;

c) désigner le poste d'AE responsable du système d'enregistrements ou désigner un poste existant dont le titulaire se voit confier la même responsabilité par la haute direction;

d) stipuler que le système d'enregistrements sera conforme au manuel sur la GE, à la législation et aux normes nationales et normes de l'industrie de façon à ce que les enregistrements produits et/ou mis en mémoire par le système soient toujours admissibles en preuve;

e) confier à l'AE la responsabilité de tenir à jour et de modifier le manuel sur la GE avec l'appui du personnel de la TI de façon à ce que le manuel reflète continuellement l'état précis du système d'enregistrements et puisse être utilisé comme preuve de la conformité du système avec la législation et la présente norme;

f) énumérer les exigences de haut niveau relatives à la création, à la gestion, à l'utilisation, à la destruction, au transfert ou à la préservation des enregistrements;

g) veiller à ce que le personnel de la TI travaille avec l'AE pour intégrer la gestion des enregistrements dans le cours usuel et ordinaire des affaires de l'organisation et maintenir cette intégration;

h) définir les responsabilités de l'AE en matière d'assurance de la qualité des enregistrements et de surveillance de la conformité avec le soutien du personnel de la TI.

6.3.3 Conformité à la politique de GE

La conformité à la politique nécessite les éléments suivants :

a) l'autorisation de la personne (un particulier ou le titulaire d'un poste) responsable de l'obtention et de la préservation de cette conformité;

b) le recensement des lois, directives et règlements pertinents auxquels l'organisation se conformera;

c) le recensement des normes nationales ou internationales pertinentes ou des dispositions desdites normes nationales ou internationales auxquelles l'organisation se conformera;

d) une évaluation de la façon dont l'organisation se conforme à l'ensemble des directives, lois et règlements applicables.

Les documents mentionnés ci-dessus seront notés dans la politique de GE. Des audits périodiques doivent être menés pour vérifier la conformité.

6.4 Manuel sur la gestion des enregistrements

6.4.1 Généralités

La mise en œuvre d'un programme de GE nécessite l'utilisation d'un manuel sur la gestion des enregistrements (manuel sur la GE) qui consolide toutes les procédures se rapportant aux enregistrements, pour faire en sorte qu'elles soient uniformes et complètes. Le manuel sur la GE doit être conforme à la politique de GE et à toutes les normes indiquées.

Le manuel sur la GE doit décrire les procédures de production, de réception, de saisie, de gestion, d'utilisation, de protection, de destruction et de préservation des enregistrements tout au long de leur cycle de vie. Les changements apportés aux procédures de GE seront autorisés, documentés, distribués et inclus dans le manuel.

Le manuel sur la GE doit être tenu à jour et refléter fidèlement la nature exacte, les fonctions, les procédures et les processus du système d'enregistrements de l'organisation, c'est-à-dire la façon dont ce système participe au cours usuel et ordinaire des affaires et l'appuie, ainsi que la façon avec laquelle les changements rapides sur le plan technologique ont des incidences sur les procédures et les processus.

Le manuel sur la GE doit définir le fonctionnement et l'utilisation du système d'enregistrements et comprendra des renvois à d'autres documents pertinents (p. ex., d'autres manuels de procédures, des procédures opérationnelles, de la documentation sur le système de la TI) le cas échéant. Le manuel sur la GE doit comprendre un cycle d'examen formel pour faire en sorte qu'il demeure harmonisé aux autres exigences organisationnelles.

6.4.2 Saisie des enregistrements

6.4.2.1 Généralités

Les enregistrements peuvent être produits par l'organisation ou importés dans son système d'enregistrements à partir d'une source externe. Le manuel sur la GE doit documenter les procédures de contrôle pour la saisie et les niveaux d'assurance de la qualité pour faire en sorte que les enregistrements saisis soient exacts et afin de vérifier l'intégralité des enregistrements et des métadonnées. Le manuel doit également documenter les procédures utilisées pour les enregistrements de toute forme, y compris les enregistrements non textuels (p. ex., audio, images, vidéo et multimédia).

Le manuel sur la GE doit définir des procédures permettant d'appliquer des contrôles systématiques des versions à tous les enregistrements. La responsabilité de remplacer les enregistrements mis en mémoire par leurs nouvelles versions doit être documentée dans la documentation du système ainsi que les procédures connexes. Une procédure de contrôle des versions doit être établie pour tous les enregistrements.

Lorsque des systèmes de gestion du flux de travail sont mis en place, les détails opérationnels et les procédures de contrôle des changements doivent être documentés dans le manuel sur la GE. Ces renseignements permettront de veiller à ce que l'intégrité des enregistrements ne soit pas compromise pendant un processus de gestion du flux de travail et que les enregistrements ne se perdent pas.

6.4.2.2 Métadonnées

Les métadonnées sont des données servant à définir le contenu, le contexte et la structure des enregistrements et à en décrire l'utilisation, la gestion, l'historique de conservation et les changements technologiques.

Au Canada, la législation ne prescrit pas un nombre minimal de métadonnées pour les preuves électroniques présentées dans le cadre de procédures judiciaires ni de poids précis en tant que preuve documentaire. Les métadonnées sont gérées au cas par cas par les tribunaux canadiens. Toutefois, la création et la gestion des

métadonnées font partie intégrante de la gestion des enregistrements, permettent d'identifier, d'enregistrer, de classifier, d'accéder, de découvrir, de disposer, de préserver, de prouver l'intégrité et l'authenticité des enregistrements, d'assurer le contrôle des versions, etc. Les métadonnées permettent d'assurer l'authenticité (identité et intégrité), la fiabilité et l'utilisabilité des enregistrements au fil du temps.

La production, la gestion, la disposition et la préservation des métadonnées devraient être formellement autorisées par l'organisation dans le manuel sur la GE. Le manuel devrait préciser que les métadonnées :

a) sont des renseignements au sujet d'un enregistrement, peu importe le support, qui servent à identifier, à décrire, à gérer, à authentifier, à comprendre et à interpréter l'enregistrement et à donner accès à l'enregistrement;

b) sont produites au moment de la création de l'enregistrement (c'est-à-dire lorsque l'enregistrement est produit ou reçu ou mis en mémoire dans un regroupement d'enregistrements). Les métadonnées continuent de s'accumuler pendant le cycle de vie de l'enregistrement;

c) font partie intégrante de l'enregistrement, et leur production et leur gestion font partie intégrante du système d'enregistrements;

d) sont conservées et utilisées par le créateur des enregistrements dans le cours usuel et ordinaire des affaires et elles sont découvrables;

e) peuvent comprendre des renseignements personnels et être visées par les lois sur la protection des renseignements personnels;

f) permettent d'évaluer la crédibilité de l'enregistrement, c'est-à-dire sa fiabilité, son exactitude et son authenticité en tant que preuve.

Les métadonnées doivent être saisies ou créées afin d'identifier chaque enregistrement et d'en établir l'intégrité au moment de sa création et tout au long du cycle de vie de l'enregistrement. Les métadonnées essentielles comprennent, sans s'y limiter, les éléments suivants : le titre du document, la date de création et/ou des modifications, l'auteur, le destinataire, le type de document, etc. Les métadonnées doivent continuer de s'accumuler ou être créées de manière à assurer le suivi des changements technologiques (migration, conversion, etc.), de l'intégrité, des droits (autorisations, accès), etc.

6.4.2.3 Numérisation

La numérisation est un processus selon lequel les organisations convertissent des enregistrements analogues en enregistrements numériques. Puisque bon nombre d'enregistrements sont maintenant créés, saisis, tenus à jour, utilisés et préservés en format numérique, les organisations peuvent décider de numériser leurs enregistrements analogues afin de réduire les efforts de récupération et/ou de mettre en place des flux de travail numériques du début à la fin. La numérisation peut également réduire les exigences d'entreposage physiques et/ou améliorer la continuité des activités. Bien que les enregistrements numérisés soient acceptés par les tribunaux, des documents physiques pourraient par moment être considérés comme étant une meilleure preuve puisqu'ils sont jugés comme étant les documents originaux.

Les organisations peuvent décider de numériser l'information enregistrée dans leurs locaux et/ou d'externaliser leurs travaux de numérisation à des fournisseurs de services externes. Lorsque la numérisation est effectuée dans les locaux de l'organisation, cette tâche peut être accomplie de façon centralisée à l'aide de matériel spécialisé exploité par des techniciens qualifiés. Elle peut également être répartie entre des employés à l'échelle de l'organisation et réalisée à l'aide d'appareils multifonctions ou de numériseurs de bureau afin de produire des enregistrements numérisés. Peu importe le processus de numérisation choisi, celui-ci doit s'aligner soigneusement sur les besoins opérationnels et doit être conçu pour pouvoir créer des enregistrements numériques substituts de qualité suffisamment élevée à partir d'enregistrements analogues avec des niveaux minimaux, identifiables et acceptables de perte d'information ou autre donnée, comme l'aura établi l'organisation. Les organisations doivent être en mesure d'attester que les versions numériques des enregistrements analogues sont complètes et exactes,

et qu'elles peuvent donc fournir une preuve des activités auxquelles les enregistrements sources ont servi. Ces enregistrements numériques doivent être découvrables et accessibles pour les personnes qui ont le droit d'y avoir accès, et ce, aussi longtemps que nécessaire.

Avant d'entreprendre un projet de numérisation, les organisations doivent :

a) évaluer si les enregistrements peuvent être numérisés;

b) s'assurer qu'il n'existe pas d'obstacles juridiques au remplacement d'enregistrements analogues par des enregistrements numériques;

c) déterminer si tous les enregistrements ou une partie d'entre eux devraient être numérisés;

d) s'assurer qu'un nombre suffisant de ressources humaines, matérielles et financières sont disponibles pour mener à bien le projet;

e) déterminer si la numérisation devrait être réalisée à l'interne ou confiée à un fournisseur de services externe;

f) identifier lesquels des enregistrements analogues ou numérisés sont les enregistrements officiels;

g) déterminer si les enregistrements sources devront être conservés ou détruits.

Le manuel sur la GE doit exposer les procédures et les processus permettant d'obtenir des reproductions exactes et lisibles des enregistrements sources, de même que des métadonnées appropriées aux fins de la gestion et de l'extraction des enregistrements. L'assurance de la qualité doit être menée et certifiée par l'organisation, et les enregistrements sources ne doivent pas être détruits, même si leur destruction est autorisée, tant que les procédures d'assurance de la qualité ne seront pas terminées et que toutes les corrections n'auront pas été documentées.

Le manuel sur la GE doit renfermer une liste des enregistrements analogues dont la numérisation est approuvée par l'organisation et documentera les motifs juridiques et opérationnels justifiant la destruction autorisée de tout enregistrement source. Si, après la numérisation, les enregistrements papiers sont habituellement détruits, les copies numérisées deviennent alors des enregistrements authentiques et faisant autorité qui peuvent être utilisés à des fins commerciales et juridiques. L'authenticité, la fiabilité et l'intégrité de ces enregistrements doivent être confirmées en s'assurant qu'ils respectent les exigences relatives à la numérisation énoncées dans le manuel sur la GE. L'intégrité du système peut être validée selon l'emplacement où les enregistrements numérisés sont mis en mémoire et administrés (voir l'art. 31.1 et l'art. 31.5 de la LPC).

6.4.3 Classification et indexation

La classification et l'indexation sont des composantes clés de tout programme de GE, en ce sens qu'ils permettent d'organiser logiquement les enregistrements et d'en assurer l'identification, le contrôle, l'extraction et la disposition. Tous les enregistrements devraient être classifiés de façon à pouvoir être replacés dans leur contexte documentaire et indexés pour que l'extraction en soit facilitée. En ce qui concerne les enregistrements électroniques, ces fonctions sont mises en œuvre à l'aide des métadonnées. Les éléments suivants devront être clairement indiqués dans le manuel sur la GE :

a) la méthodologie de classification utilisée est précisée (p. ex., classification fonctionnelle) et le système de classification est illustré au moyen d'un schéma;

b) le type et la structure d'indexation utilisés, y compris le critère d'indexation principal et tout autre niveau d'indexation;

c) la procédure de mise à jour du schéma de classification et de l'index;

d) la procédure de correction des catégories, codes ou entrées d'index inexacts;

e) la procédure de mise en œuvre de c) et d);

f) des méthodes permettant de faire le suivi du statut des codes de classification et des entrées d'index qui ont été mis à jour, supprimés ou détruits;

g) la procédure d'assurance de la qualité de la classification et de l'indexation.

6.4.4 Tenue à jour et utilisation des enregistrements

L'AE doit superviser et coordonner toutes les activités visant à s'assurer que les enregistrements dans le système d'enregistrements demeurent authentiques, accessibles et sécurisés.

L'AE doit tenir à jour un registre des autorisations d'extraire, de lire, d'annoter, de modifier, de transmettre et de supprimer des enregistrements (en d'autres termes, les privilèges d'accès) qui sont accordées aux agents et aux employés de l'organisation. L'AE doit s'assurer que la nature de toute action entreprise à l'égard des enregistrements est documentée, que ce soit par l'ajout de métadonnées relatives à l'intégrité ou par la compilation de rapports, et ce, afin de constituer une piste de vérification (voir 6.5.5) de ce qui est arrivé aux enregistrements depuis leur création. Cette information est nécessaire pour évaluer la crédibilité continue des enregistrements dans le système.

6.4.5 Exigences relatives à la conservation des enregistrements

La période de conservation des enregistrements doit être déterminée par les personnes ou les titulaires des postes autorisés au sein de l'organisation, y compris les responsables des fonctions organisationnelles qui reposent sur les enregistrements, c'est-à-dire le conseiller juridique (pour assurer le respect des lois), le responsable des finances (pour assurer le respect des exigences financières) et l'AE (pour veiller à ce que les décisions concernant la conservation et la disposition s'inspirent de méthodes et de principes judicieux en matière de gestion et de préservation des enregistrements). Les exigences relatives à la conservation des enregistrements doivent être documentées dans le calendrier de conservation des enregistrements de l'organisation, qui devrait être relié au schéma de classification des enregistrements. L'attribution de la responsabilité de déterminer les exigences en matière de conservation des enregistrements à des personnes ou à des titulaires de poste (p. ex., l'AE) doit être formellement documentée.

Les périodes de conservation sont habituellement déterminées en fonction de la valeur des enregistrements et du besoin de l'organisation d'y accéder ainsi que par d'autres exigences se rapportant à la valeur probante, à la gestion des risques, aux lois et aux audits. C'est à l'AE de l'organisation qu'incombe la responsabilité de veiller à ce qu'une évaluation en bonne et due forme soit faite des enregistrements en fonction des éléments suivants :

a) la façon dont les enregistrements sont utilisés par l'organisation (à l'interne et à l'externe);

b) le besoin des usagers d'avoir accès aux enregistrements en cas de sinistre;

c) la valeur financière, juridique, sociale, politique et historique des enregistrements;

d) l'analyse coûts-avantages de la conservation des enregistrements;

e) les conséquences que représentera pour l'organisation la destruction des enregistrements;

f) la valeur probante des enregistrements en cas de poursuite, d'audit ou d'investigation.

Une fois la valeur de chaque ensemble (classe ou catégorie) d'enregistrements établie, l'AE documentera la durée de conservation des enregistrements et la façon de les transférer au gardien désigné (pour une période déterminée ou à des fins de conservation permanente), ou comment les détruire une fois qu'ils ne sont plus nécessaires.

Que l'organisation ait besoin de conserver les enregistrements pendant des périodes brèves ou longues ou indéfiniment, elle doit veiller à ce que l'environnement technologique soit susceptible d'assurer cette conservation

(p. ex., jusqu'à telle date ou jusqu'à tel événement ou en permanence). De plus, avant que la décision de détruire (ou de transférer) les enregistrements soit mise en œuvre, elle doit être passée en revue par l'AE, au cas où une mise en suspens pour des raisons juridiques s'imposerait (voir 5.4) ou qu'un événement se soit produit qui nécessite une période de conservation plus longue.

La politique de gestion des enregistrements de l'organisation doit définir également les « enregistrements temporaires » – c'est-à-dire les enregistrements auxquels aucune exigence en matière de conservation ne s'applique et qui ne revêtent pas d'intérêt pour documenter ou justifier l'activité de l'organisation.

6.4.6 Disposition des enregistrements

6.4.6.1 Généralités

Par « disposition », on entend la mesure prise relativement à un enregistrement à l'expiration de sa période de conservation : destruction ou transfert. Réalisée en conformité avec un calendrier de conservation et de disposition des enregistrements, la disposition est considérée comme faisant partie intégrante du cours usuel et ordinaire des affaires de l'organisation. Le manuel sur la GE doit stipuler que toutes les dispositions doivent être documentées. L'AE aura le pouvoir de suspendre la destruction ou le transfert d'enregistrements faisant l'objet d'une mise en suspens pour des raisons juridiques (voir 5.4) ou d'examen ou d'audit à l'intérieur de l'organisation ou à l'échelle gouvernementale.

6.4.6.2 Processus de disposition

Le manuel sur la GE doit stipuler que la disposition des enregistrements a lieu lorsque la période de conservation appropriée est terminée, que la disposition a été autorisée et que tout obstacle à l'élimination a été levé. L'organisation doit être en mesure de présenter de la documentation relativement à la disposition de ses enregistrements lorsque la preuve en est justifiée ou exigée en fonction d'exigences opérationnelles ou des exigences de la loi ou d'un audit. Cette documentation devrait indiquer quels enregistrements ont été éliminés au moyen des métadonnées connexes (p. ex., code de classification, dates inclusives, bureau de première responsabilité), l'organisation qui a autorisé la disposition et le moment où la disposition a eu lieu. L'organisation doit conserver en permanence ce registre des mesures de disposition à titre de preuve.

Le manuel sur la GE peut stipuler que les métadonnées doivent être conservées même après la disposition des enregistrements auxquels elles se rapportent; la disposition sera alors enregistrée dans les métadonnées. Si un enregistrement électronique est associé à plus d'un regroupement d'enregistrements, il pourra être éliminé dans le contexte d'un regroupement, mais conservé dans le contexte d'un autre regroupement; dans ce cas, la disposition consistera à supprimer de l'enregistrement les métadonnées associées à l'ensemble d'enregistrements qui est éliminé.

6.4.6.3 Destruction d'enregistrements électroniques

Il peut arriver que les registres des transactions dans le système, les pistes de vérification et d'autres enregistrements appropriés d'activités de destruction et de modification doivent être conservés en permanence. Ils pourront se révéler nécessaires pour détruire un enregistrement particulier dans un système d'enregistrements en raison d'exigences juridiques ou administratives, particulièrement en conformité de la réglementation sur la protection des renseignements personnels ou d'autres lois. Le manuel sur la GE doit stipuler qu'un processus modifiable de destruction, de modification ou de correction des enregistrements peut être utilisé dans le système d'enregistrements. Lorsqu'un enregistrement est détruit, les procédures du système permettront de s'assurer que l'enregistrement et le locateur d'enregistrement soient détruits. La destruction d'enregistrements électroniques se fera de telle façon que la confidentialité des enregistrements est préservée et que les renseignements personnels ne sont pas divulgués.

6.4.6.4 Transfert des enregistrements électroniques à une autre entité

Le manuel sur la GE doit stipuler que les enregistrements transférés à un gardien désigné et acceptés par ce dernier (p. ex., un service d'archives) apparaîtront dans la documentation de l'organisme cédant et dans celle de

l'organisme cessionnaire. Le manuel pourra aussi exiger que soient indiqués le matériel et le ou les logiciels à partir desquels les enregistrements ont été produits ainsi que la documentation de programme qui décrit le format, les codes de fichier, les clichés d'enregistrement et d'autres caractéristiques techniques du système d'enregistrements dans lequel les enregistrements étaient conservés.

6.4.7 Préservation des enregistrements

Le manuel sur la GE doit indiquer que dans l'environnement numérique, la préservation commence par la création contrôlée et la tenue à jour des enregistrements dans des formats de fichier conservables assortis des métadonnées d'identité et de tenue de documents essentielles requises pour démontrer qu'un enregistrement a été produit ou reçu ou mis en mémoire dans le cours usuel et ordinaire des affaires, est authentique et a été tenu à jour adéquatement dans le système d'enregistrements sans modifications non autorisées.

Le système d'enregistrements de l'organisation doit avoir la capacité de conserver de manière permanente les enregistrements qui revêtent une valeur permanente pour leur créateur. Les enregistrements créés par les organisations peuvent présenter une valeur permanente et répondre aux conditions de préservation permanente et doivent être protégés contre l'obsolescence des logiciels.

6.4.7.1 Conversion et migration des enregistrements

Le manuel sur la GE doit donner des consignes sur la conversion et la migration. La conversion et la migration des enregistrements sont des méthodes utilisées pour contrer l'obsolescence des logiciels qui fait que les enregistrements électroniques deviennent inaccessibles au fil du temps. Il y a deux types d'obsolescence des enregistrements numériques : l'obsolescence des formats de fichier, c'est-à-dire lorsqu'il n'y a plus d'applications logicielles permettant d'ouvrir un enregistrement numérique ou d'en visualiser le contenu; et l'obsolescence des systèmes, lorsque le système ou l'application n'est plus pris en charge (dans certains cas en raison de l'obsolescence du matériel) et qu'il est impossible de récupérer, d'ouvrir ou de visualiser les enregistrements. Pour régler le problème de l'obsolescence des formats de fichier, on aura recours à la conversion des fichiers, c'est-à-dire le transfert de l'enregistrement d'un format à un autre (l'application d'origine ou le fichier source sera aussi conservé). Pour régler le problème de l'obsolescence des systèmes, les fichiers numériques seront transférés à un nouveau système ou à une nouvelle application (on pourra souvent faire appel dans ce cas à la virtualisation de système) ou, dans de rares cas, l'ancien matériel sera conservé ou un logiciel spécialisé permettant d'accéder aux médias obsolètes sera acquis.

La conversion et la migration représentent toujours des risques et avant de les entreprendre, l'organisation doit déterminer les fonctionnalités requises de l'ancien format et celles qui doivent être préservées dans le nouveau format et le nouveau système et elle documentera ces décisions, car différents logiciels peuvent produire un même enregistrement de différentes façons. Quel que soit le format de préservation choisi, la conversion et la migration doivent être intégrées dans un processus opérationnel bien documenté qui s'inscrit dans l'exploitation régulière du système d'enregistrements.

Les organisations doivent avoir une politique de conversion et de migration et le manuel sur la GE doit exposer des procédures détaillées permettant de faire en sorte que la structure, le contenu, les métadonnées d'identité et de tenue de documents et, dans le cas de courriels, les pièces jointes, hyperliens, preuves de livraison, listes de distribution et relation avec d'autres enregistrements de l'organisation à l'intérieur et à l'extérieur de l'organisation, sont protégés et préservés. Une somme de contrôle permettant de vérifier qu'il n'y a pas eu d'erreur dans la conversion ou la migration devrait être exigée pour chaque fichier.

6.4.7.2 Formats de préservation

Le manuel sur la GE doit indiquer les formats préférés par l'organisation à des fins de préservation selon le type d'enregistrement. Il existe diverses ressources pour faciliter la sélection des formats appropriés de préservation et l'exécution de la conversion. Le choix des formats de préservation dépendra du nombre de changements qui peuvent encore être faits avant que la représentation de l'enregistrement soit trop dégradée pour tenir lieu de copie fiable de l'enregistrement dans son format d'origine dans le cadre d'une procédure judiciaire.

6.4.8 Assurance de la qualité

Essentiellement, un programme de gestion des enregistrements est un programme d'assurance de la qualité conçu pour appuyer la création, la gestion, l'utilisation, la disposition et la préservation d'enregistrements crédibles qui fournissent la preuve des activités de l'organisation dans le cours usuel et ordinaire des affaires. Même si la politique et le manuel de gestion des enregistrements documentent les contrôles que l'organisation a mis en place pour appuyer l'intégrité des enregistrements et du système, un mécanisme d'assurance de la qualité est nécessaire pour veiller à ce que le programme de gestion des enregistrements de l'organisation se conforme aux exigences législatives, administratives, opérationnelles et techniques et les respecte systématiquement et que les fraudes ou les abus soient évités ou détectés et que des mesures soient prises pour les contrer le plus rapidement possible.

L'assurance de la qualité signifie que l'organisation définit le niveau approprié de service et veille à ce que les membres du personnel comprennent leurs rôles et leurs responsabilités et reçoivent la formation nécessaire pour dispenser ce niveau de service. À cette fin, l'AE mettra en œuvre des processus appropriés d'assurance de la qualité, y compris, mais sans s'y limiter, une surveillance du rendement et de la conformité, des auto-évaluations, des audits externes et des procédures à suivre en cas d'incident, en plus de noter et de certifier que toutes les fonctions de GE sont remplies. L'AE doit signaler immédiatement tout enjeu significatif au cadre supérieur dont relève le programme, qui prendra les mesures nécessaires et ordonnera que soient apportés les rajustements requis au programme de GE et/ou approuvera ces rajustements.

7 Gestion du système de la TI

7.1 Généralités

Tous les éléments importants de l'architecture logique et physique du système de la TI où sont conservés les enregistrements doivent être intégralement documentés dans un guide de gestion du système de la TI, y compris les responsabilités et les relations entre la gestion du système de la TI, le programme de GE et la conduite des affaires de l'organisation. Le guide de gestion du système de la TI doit être structuré de telle sorte que l'intégrité du système puisse être démontrée pour n'importe quel moment dans le temps.

La documentation requise pour le système de la TI doit comprendre les éléments suivants :

a) description du matériel ainsi que des éléments réseau du système et la façon dont ils interagissent;

b) description des systèmes d'exploitation et des logiciels d'applications, y compris les formats d'enregistrement;

c) description des mesures de protection de la sécurité de la TI, comme les pare-feux, les copies de sauvegarde du système et les mesures de reprise après sinistre;

d) description des procédures de vérification de l'intégrité du système, y compris l'ordonnancement des événements et les obligations redditionnelles, pour la surveillance et la maintenance des systèmes et l'intégrité des données et pour la prise de mesures préventives et correctives, le cas échéant;

e) registres des problèmes, calendriers et procédures pour évaluer l'intégrité opérationnelle continue du système et pour prendre des mesures correctives, le cas échéant;

f) évaluation des risques et des répercussions associés à l'intégrité du système et des données à la suite de défaillances techniques soudaines, inhabituelles ou d'une panne majeure dans le fonctionnement du système d'enregistrements ou du système de la TI connexe, lorsque ces derniers ne fonctionnent pas comme prévu ni conformément aux spécifications;

g) documentation des changements apportés au système, y compris l'évaluation des risques et des répercussions sur l'intégrité des données et du système, y compris toutes les personnes ou les postes responsables et un relevé complet des activités et des processus mis en œuvre pour opérer le changement;

h) procédures pour contrôler l'utilisation du matériel et des logiciels de maintenance du système qui peuvent contourner les contrôles d'accès au système, ainsi que les autorisations nécessaires pour leur utilisation.

Le gestionnaire responsable du système de TI doit veiller à ce que le guide de gestion du système de la TI soit tenu à jour.

7.2 Évaluation des risques liés à la technologie

Il arrive de plus en plus souvent que les organisations créent, gèrent et utilisent des enregistrements dans une variété de systèmes, de services et de dispositifs. L'information enregistrée peut être accessible de n'importe où, ce qui peut présenter des enjeux sur le plan de la sécurité, notamment il y a des risques qu'elle soit utilisée hors de son contexte, qu'elle soit copiée, modifiée, manipulée, piratée ou encore falsifiée. Par conséquent, les avantages et les risques associés à l'adoption de nouvelles technologies doivent être recensés dans le cadre d'un processus d'évaluation des risques.

L'évaluation des risques est un outil permettant de définir, de classifier et de jauger les risques et elle fournit de l'information à utiliser dans l'élaboration de stratégies et de politiques d'atténuation des risques, particulièrement ceux associés aux nouvelles technologies. L'organisation doit soigneusement examiner les incidences juridiques complexes des nouvelles technologies au moyen d'une approche multidisciplinaire (p. ex., aspects juridiques, sécurité, protection des renseignements personnels, TI, gestion des risques, etc.) qui tient compte de son infrastructure existante et de sa tolérance aux risques.

Avant de procéder à l'adoption une nouvelle technologie, l'organisation doit :

a) constituer une équipe d'évaluation des risques (c'est-à-dire gestionnaire des risques, spécialiste de l'architecture organisationnelle de la TI, analyste de réseau de la TI, expert juridique, agent de sécurité et AE) qui examinera la nouvelle technologie et présentera des recommandations au sujet de son adoption;

b) faire référence au cadre de gestion des risques existant de l'organisation (c'est-à-dire politique, procédures et lignes directrices);

c) désigner les intervenants et les cas d'utilisation;

d) définir, évaluer et atténuer les menaces et risques associés à la nouvelle technologie;

e) veiller à ce que des mécanismes soient en place pour rendre compte à la haute direction, et à ce que la haute direction ait rendu sa décision avant l'adoption de la nouvelle technologie;

f) élaborer une politique et des procédures documentées pour la nouvelle technologie (ce qui comprendra la mise à jour du manuel sur la GE et du guide de gestion du système de la TI);

g) communiquer au personnel la politique et les procédures concernant la nouvelle technologie.

Dans les provinces où les institutions gouvernementales sont assujetties aux exigences en matière d'évaluation des répercussions sur la vie privée, l'évaluation des risques et des répercussions sur la protection des renseignements personnels peuvent être combinés.

Les technologies pour lesquelles une évaluation des risques est nécessaire comprennent, sans toutefois s'y limiter, les appareils mobiles, les plates-formes de médias sociaux, les systèmes d'intelligence artificielle et les systèmes décisionnels automatisés.

7.2.1 Appareils mobiles

Les organisations qui permettent à leurs employés d'utiliser leurs propres appareils pour s'acquitter de leurs fonctions doivent mener une évaluation des risques afin de tenir compte des enjeux découlant de l'utilisation « sans

frontière » de ces appareils, notamment en ce qui a trait aux licences de bases de données et de logiciels, de sécurité, de protection des renseignements personnels, de propriété intellectuelle et de loi sur l'emploi.

Après avoir mené une évaluation des risques, l'organisation diffusera une politique clairement définie et strictement applicable relative à l'utilisation des appareils personnels, notamment :

a) si l'utilisation d'appareils personnels dans le cadre du travail est autorisée;

b) les types d'appareils qui sont autorisés;

c) les responsabilités de l'employeur et de l'employé relativement à l'utilisation des appareils, y compris les procédures en place lorsqu'un employé quitte l'organisation;

d) la façon dont les enregistrements liés au travail seront gérés et transférés dans le système de tenue des enregistrements de l'organisation.

7.2.2 Médias sociaux

Lorsqu'une organisation a recours aux médias sociaux, cela soulève des enjeux en matière de preuve, notamment des points de vue suivants :

a) l'identification des enregistrements;

b) la détermination de leur auteur et de leur propriétaire (ce qui est nécessaire pour établir à qui il incombe d'identifier, de saisir et de gérer l'enregistrement);

c) la définition de leur contexte (et par conséquent, la capacité de déterminer s'ils ont été générés dans le cours usuel et ordinaire des affaires);

d) l'évaluation de leur fiabilité, de leur exactitude et de leur authenticité;

e) l'identification d'une chaîne de possession (particulièrement si certaines personnes téléchargent des enregistrements commerciaux vers leurs propres pages de médias sociaux ou les pages d'autres personnes).

Les organisations doivent se doter d'une politique sur les médias sociaux qui définira :

a) le moment à partir duquel une publication est considérée comme un enregistrement;

b) le processus par lequel les enregistrements sont capturés, y compris la création d'une copie authentique assortie de métadonnées d'identité indiquant clairement le contexte d'affichage, qui en est responsable et les actions connexes qu'il y a pu y avoir.

Les enregistrements existants de l'organisation qui sont affichés dans les médias sociaux en tant que liens doivent être mis en mémoire par l'organisation conformément au calendrier de classification, d'indexation, de conservation et de disposition, en tenant compte, toutefois, que les fournisseurs de médias sociaux conservent de tels enregistrements indéfiniment.

Si une poursuite est possible, voire anticipée, il pourra être nécessaire de prendre des clichés ou des images additionnels du matériel pertinent, étant donné que les sites des médias sociaux peuvent être fermés, que des comptes peuvent être fermés ou des abonnements résiliés, et que le contenu peut être supprimé.

7.2.3 Intelligence artificielle et systèmes décisionnels automatisés

Les enregistrements sont de plus en plus créés, accessibles, utilisés et analysés au moyen de systèmes d'intelligence artificielle (IA) complexes et de systèmes décisionnels automatisés (SDA). Au Canada, la réglementation des systèmes d'IA est toujours en cours d'élaboration.[4]

Les enjeux juridiques et éthiques qui doivent être pris en compte lorsqu'un système d'IA est utilisé comprennent, sans toutefois s'y limiter, ce qui suit :

a) biais (données, algorithmes, humains);

b) manque de transparence quant aux systèmes et processus d'IA, y compris la façon dont les systèmes d'IA ont été entraînés;

c) manque d'explications sur les systèmes et processus d'IA, y compris sur la façon dont les systèmes d'IA ont été entraînés;

d) protection et sécurité des données et renseignements personnels;

e) pertinence des enregistrements produits à partir d'un système d'IA et présentés comme preuves documentaires;

f) l'authenticité, l'intégrité et la validité des enregistrements ou résultats produits avec l'IA.

Si une organisation utilise l'IA ou un système décisionnel automatisé, elle devrait effectuer une évaluation des risques et déterminer comment elle pourra démontrer que le système produit des résultats exacts et fiables (c.-à-d. cohérents).

7.3 Copies de sauvegarde et reprise du système

Des procédures efficaces pour la réalisation de copies de sauvegarde des enregistrements électroniques et de toute l'information connexe (p. ex., fichiers index et pistes de vérification) ainsi que pour la reprise du système doivent figurer dans le guide de gestion du système de la TI. Seules les personnes autorisées pourront activer ou désactiver les fonctions de copies de sauvegarde et de reprise.

Le guide de gestion du système de la TI doit stipuler que les supports de mise en mémoire devront être testés pour prouver qu'aucune information enregistrée ni aucune métadonnée n'a été perdue ou remplacée et que l'exactitude et l'intégrité des copies de sauvegarde seront testées à des intervalles prédéterminés.

Un registre des sauvegardes doit être conservé dans la piste de vérification du système et il fera état de toutes les activités de sauvegarde et de reprise, y compris de tout problème qui a surgi pendant la procédure. Il est prudent d'avoir plusieurs copies de sauvegarde simultanées de l'information enregistrée et des programmes d'application et d'en conserver une hors site. Le guide de gestion du système de la TI doit comprendre les procédures de transport des copies de sauvegarde d'un site à un autre.

Si la structure des fichiers de données conservés sur une copie de sauvegarde diffère de celle des enregistrements électroniques, les différences doivent être documentées.

Le guide de gestion du système de la TI doit stipuler que lorsque des fichiers de données de sauvegarde sont utilisés aux fins de reprise après une panne de système, les procédures seront documentées pour confirmer que

---

[4] Voir les principes ambitieux de haut niveau définis dans la déclaration suivante : https://www.declarationmontreal-iaresponsable.com/ (2018, Université de Montréal). De plus amples renseignements sont disponibles à https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32592 (2019, Conseil du Trésor du Canada). Le projet de loi C-27 (la *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, y compris la *Loi sur l'intelligence artificielle et les données*), déposé le 16 juin 2022, constituerait la première loi qui établirait de nouvelles règles concernant le développement et le déploiement responsable de l'intelligence artificielle au Canada.

l'intégrité des fichiers de données n'a pas été compromise. Le manuel doit également stipuler que les procédures de sauvegarde et des détails au sujet des transferts seront conservés aussi longtemps que les enregistrements de référence sont nécessaires.

Les aspects technologiques des copies de sauvegarde et de reprise du système seront couverts par le guide de gestion du système de la TI. La création de miroirs et la redondance peuvent remplacer les copies de sauvegarde en cas de catastrophe.

Les copies de sauvegarde sont un produit de la fonction de sécurité d'une organisation et devraient être éliminées régulièrement, par rotation, selon un terme explicitement défini.

7.4 Sécurité et protection

7.4.1 Politique et procédures de sécurité de la TI

L'organisation doit avoir une politique de sécurité de la TI précisant les niveaux d'accès au système d'enregistrements (c'est-à-dire l'ensemble des enregistrements de l'organisation et les systèmes connexes de gestion et de préservation des enregistrements), ainsi que les niveaux de protection du système de la TI (c'est-à-dire la totalité des ordinateurs, logiciels et dispositifs de l'organisation utilisés pour traiter et transformer l'information.

Des procédures doivent être mises en œuvre conformément à la politique de sécurité de la TI de l'organisation. Ces procédures comprendront la définition des contrôles d'authentification des usagers et d'autorisation à l'échelle du système, les utilisateurs privilégiés et la notification des accès non autorisés et des mesures de protection pour les contrer, ainsi que des lignes directrices sur l'accès et les changements dans le personnel autorisé à accéder au système. Le filtrage de sécurité des personnes qui travaillent pour l'organisation doit se faire selon le niveau de confidentialité de l'information. L'environnement d'hébergement et d'exploitation aux fins de la mise en mémoire, du transport et de l'entretien de supports de mise en mémoire doit être conforme aux normes nationales ou internationales pertinentes.

7.4.2 Clés de chiffrement et signatures électroniques sécurisées

Lorsqu'il s'impose d'assurer la sauvegarde de l'information enregistrée, un système de chiffrement doit être utilisé pour améliorer la sécurité et assurer l'intégrité de l'information enregistrée pendant la transmission et la mise en mémoire.

Lorsque des signatures électroniques sécurisées sont utilisées, des procédures doivent être mises en œuvre pour l'attribution et la gestion des clés de chiffrement et la gestion des certificats. Les clés de chiffrement ou de signature électronique doivent être valides, conservées en lieu sûr et mises à la disposition des personnes autorisées seulement.

7.4.3 Horodatage

La vérification régulière des horloges des ordinateurs pour confirmer l'exactitude de la date et de l'heure doit être documentée. L'horodatage nécessite que les erreurs de date et d'heure puissent être repérées et corrigées. Toutes les mesures prises pour corriger les erreurs et remettre les horloges à l'heure dans tous les systèmes et dispositifs doivent être documentées.

L'organisation doit désigner les personnes autorisées à accéder aux horloges des ordinateurs et à les modifier et veillera à ce que des mesures appropriées de contrôle de l'accès soient établies.

7.5 Piste de vérification

7.5.1 Généralités

Les données d'audit représentent l'historique de chaque enregistrement et des métadonnées associées. Les données d'audit sont la preuve définitive que certains événements et certaines transactions ont eu lieu. C'est pourquoi des données d'audit doivent être saisies continuellement et qu'elles doivent toujours être protégées contre l'altération et la perte. Les données d'audit sont enregistrées dans une piste de vérification.

Les pistes de vérification doivent renfermer les données d'audit suffisantes et nécessaires pour fournir la preuve de l'authenticité des enregistrements faits par l'organisation et de l'intégrité de tout enregistrement reçu dès le moment de sa réception. La piste de vérification d'un système de la TI doit être composée de registres générés par le système et générés par l'opérateur qui renferment des données au sujet de la saisie des enregistrements mis en mémoires dans le système et des changements qui leur ont été apportés (p. ex., modification, suppression, accès). L'intégrité de la piste de vérification est importante pour satisfaire à la règle de la meilleure preuve, comme le stipulent les dispositions concernant les enregistrements électroniques des lois sur la preuve, et pour établir le poids à accorder aux enregistrements (c'est-à-dire leur valeur probante et leur caractère convaincant à titre d'enregistrements fiables).

Les procédures régissant les pistes de vérification doivent être documentées dans le guide de gestion du système de la TI.

7.5.2 Gestion des enregistrements constituant la piste de vérification

Les registres de piste de vérification doivent être assujettis à des procédures de gestion interne des enregistrements semblables à celles qui régissent d'autres enregistrements essentiels de l'organisation et doivent figurer à titre de type de document spécifique dans le guide de gestion du système de la TI. Des dispositions doivent être prises pour que les données de la piste de vérification conservées dans le système d'enregistrements soient inaltérables dans l'environnement sécurisé. Des copies de sauvegarde sécurisées de la piste de vérification doivent être conservées.

7.5.3 Contenu de la piste de vérification

L'organisation doit déterminer le contenu de la piste de vérification.

Les exigences suivantes représentent un minimum en ce qui concerne le contenu de la piste de vérification :

a) l'identification de l'information enregistrée à laquelle l'action s'est appliquée (y compris ses identificateurs uniques);

b) la personne ou le titulaire du poste responsable d'amorcer l'action et la mener à bien;

c) la date et l'heure d'événements comme les suivants :

   1) saisie initiale de l'enregistrement électronique ou d'un élément de donnée dans le système;

   2) création de nouvelles versions d'un enregistrement électronique;

   3) création, modification ou suppression de métadonnées;

   4) changements dans les autorisations d'accès aux enregistrements ou aux données;

   5) changements dans les exigences de conservation et de disposition;

   6) attribution d'une classification de sécurité à l'enregistrement ou modification de cette classification;

7) modification, destruction ou transfert d'enregistrements ou de données.

7.5.4 Création de la piste de vérification

Les données de la piste de vérification doivent être générées automatiquement par le système de la TI. Si elles ne le sont pas, les procédures utilisées pour générer les données de la piste de vérification doivent être documentées dans le guide de gestion du système de la TI et elles doivent s'appliquer à l'organisation et à tout fournisseur de services externe contractuel.

Pour les enregistrements destinés à être conservés de façon permanente, le conservateur désigné doit avoir accès aux données de la piste de vérification pour vérifier l'authenticité des enregistrements.

7.5.5 Accès

Les procédures d'accès aux données de la piste de vérification et les autorisations connexes doivent être documentées dans le guide de gestion du système de la TI.

7.5.6 Piste de vérification en matière de conversion et de migration

Si les enregistrements sont transférés d'un dispositif de stockage à un autre dans le cadre d'un processus de conversion ou de migration, les détails concernant le processus doivent être documentés dans la piste de vérification. Les procédures de migration ou de conversion doivent comprendre des méthodes démontrant que toutes métadonnées connexes sont elles aussi transférées ou converties et doivent être documentées dans le guide de gestion du système de la TI. Quand des enregistrements ont été convertis d'un format de fichier à un autre, les détails concernant la conversion doivent être documentés dans le registre de la piste de vérification.

7.5.7 Flux de travail

S'il existe des systèmes de flux de travail, le guide de gestion du système de la TI doit établir à quels points du flux de travail les données de la piste de vérification seront générées et documentées dans le système de la TI. Dans le cadre d'un système typique de flux de travail, les données de la piste de vérification sont générées à chaque étape du flux de travail.

Les données de la piste de vérification qui doivent être générées et conservées pourront changer lorsque les processus de flux de travail sont modifiés.

Le système de la TI permettra à une personne autorisée de désigner les points de la piste de vérification pour lesquels les données de la piste de vérification sont générées.

7.5.8 Vérification

Les données de la piste de vérification doivent être conservées relativement à des activités ou à des événements qui devront peut-être être reconstitués à une date ultérieure à titre de preuve supplémentaire pour renforcer la valeur probante des enregistrements électroniques.

Annexe A
(informative)
Sources de la présente norme

A.1 Introduction

La présente annexe énumère les sources qui ont été prises en considération pour la présente norme.

La norme CAN/CGSB-72.34 s'inspire de la législation en matière de preuve pour l'admission de documents (la « preuve documentaire »). Elle se concentre sur les documents pour lesquels la *Loi sur la preuve au Canada* prévoit une exception à la règle du ouï-dire, c'est-à-dire les enregistrements commerciaux. La législation sur cette question repose à la fois sur la jurisprudence (dispositions élaborées à partir de causes tranchées par les tribunaux plutôt qu'adoptées par les organismes législatifs) et sur diverses lois. La jurisprudence en matière de preuve documentaire est semblable un peu partout au Canada dans les administrations de common law. Il y a des lois sur la preuve au niveau fédéral et dans les provinces et territoires et leurs dispositions varient légèrement de l'une à l'autre. Les règles de base pour le Québec se trouvent dans le Code civil du Québec, notamment dans le Livre septième, et particulièrement aux articles 2837 à 2842, et 2870.

Aujourd'hui, la législation générale sur la preuve documentaire s'accompagne dans une grande partie du Canada par des lois particulières traitant des documents ou enregistrements électroniques.

La loi fédérale pertinente est la *Loi sur la preuve au Canada* (LPC). La LPC a été modifiée en 2000 par la Partie 3 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), en vertu de laquelle les articles 31.1 à 31.8 ont été ajoutés à la LPC.

A.2 Sources

Les sources utilisées pour la présente norme comprennent :

a) les exigences législatives au Canada, y compris celles des lois et des règlements d'application (au niveau fédéral, provincial et territorial);

b) les exigences et normes en matière de technologie, d'information et de communication (TIC);

c) les exigences en matière d'exploitation commerciale et les pratiques exemplaires (et normes connexes);

d) les exigences opérationnelles courantes des organisations ainsi que les pratiques exemplaires lorsqu'il s'agit de conserver les enregistrements et d'assurer l'intégrité de l'information figurant dans les enregistrements numériques.

Les membres du comité d'experts qui ont rédigé cette version préliminaire de la norme proviennent d'associations professionnelles et d'associations de l'industrie bien connues du Canada dans les domaines des enregistrements, de l'information et de la gestion des images; des services juridiques et financiers; et de la comptabilité et de l'audit. Les experts représentent les points de vue des usagers et des fournisseurs, pour une approche équilibrée.

Bibliographie

Les sources indiquées ci-dessous ont été examinées et prises en compte dans l'élaboration de la présente norme. Certaines sont citées en référence dans les parties informatives de la présente norme.

American National Standards Institute (ANSI). ANSI/ARMA 18-2011, *Implications of Web-Based, Collaborative Technologies in Records Management.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

American National Standards Institute (ANSI). ANSI/ARMA 19-2012, *Policy Design for Managing Electronic Messages.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

ARMA International. *Implementing Electronic Messaging Policies* (2018). Accessible à : https://www.arma.org/ (disponible en anglais seulement).

ARMA International. *Guideline for Outsourcing Records Storage to the Cloud* (2010). Accessible à : https://www.arma.org/ (disponible en anglais seulement).

Groupe CSA. CAN/CSA ISO/IEC 11179-3:2013/Amd 1:2020 *Information technology — Metadata registries (MDR) — Part 3: Registry metamodel and basic attributes.* Accessible à : https://www.csagroup.org/ (disponible en anglais seulement).

Groupe CSA. CAN/CSA ISO/IEC 14662:10 (R2020), *Technologies de l'information – Modèle de référence EDI-ouvert.* Accessible à : https://www.csagroup.org/.

Organisation internationale de normalisation (ISO). ISO 13008:2022, *Information et documentation — Processus de conversion et migration des documents d'activité numériques.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

Organisation internationale de normalisation (ISO). ISO 15489-1, *Information et documentation – Gestion des documents d'activité – Partie 1 : Concepts et principes.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

Organisation internationale de normalisation (ISO). ISO/TR 15801:2017, *Document management – Electronically stored information – Recommendations for trustworthiness and reliability*. Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

Organisation internationale de normalisation (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)*. Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

Organisation internationale de normalisation (ISO). ISO 19005-1, *Document management –Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

Organisation internationale de normalisation (ISO). ISO 19005-2, *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

Organisation internationale de normalisation (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).* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/ (disponible en anglais seulement).

Organisation internationale de normalisation (ISO). ISO 23081-1, *Information et documentation — Processus de gestion des documents d'activité — Métadonnées pour les documents d'activité — Partie 1 : Principes.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

Organisation internationale de normalisation (ISO). ISO/IEC 27001, *Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences*. Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

Organisation internationale de normalisation (ISO). ISO/IEC 27002, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

Organisation internationale de normalisation (ISO). ISO/IEC 27005, *Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information.* Accessible auprès de Standards Store par Accuris : https://global.ihs.com/.

R. v. Oler (D.M.) et al., 2014 ABPC 130 (CanLII). Accessible à : https://ca.vlex.com/vid/r-v-oler-d-681435505 (disponible en anglais seulement).

The Sedona Conference, *Les Principes de Sedona Canada concernant l'administration de la preuve électronique, troisième édition, 23e conférence de Sedona J.* 161 (2022). Accessible à : https://thesedonaconference.org/publications.