Gouvernement du Canada
Government of Canada

Office des normes générales du Canada
Canadian General Standards Board

CAN/CGSB-72.34-2017

Remplace CAN/CGSB-72.34-2005

Norme nationale du Canada

Enregistrements électroniques utilisés à titre de preuves documentaires

Office des normes générales du Canada ONGC

Conseil canadien des normes
Standards Council of Canada

Canada

Expérience et excellence
Experience and excellence
ONGC CGSB

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 aux normes à l'étude, 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 nationales. En conséquence, les normes que l'Office élabore et soumet à titre de Normes nationales du Canada se conforment aux critères et procédures établis à cette fin par le Conseil canadien des normes. Outre la publication de normes nationales, l'ONGC rédige également des normes visant 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 conformes 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 dans les cinq années 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 font l'objet de modificatifs distincts ou sont 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, et sur la façon de se les procurer figure au Catalogue de l'ONGC disponible sur notre site Web — 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 en regard de la présente norme peuvent nécessiter l'emploi de matériaux 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 canadienne 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.

Langue
Dans la présente Norme, le verbe « doit » indique une exigence obligatoire, le verbe « devrait » exprime une recommandation et le verbe « peut » exprime une option ou une permission. 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.

Pour de plus amples renseignements sur l'ONGC, ses services et les normes en général, prière de communiquer avec:

Le Gestionnaire
Division des normes
Office des normes générales du Canada
Gatineau, Canada
K1A 1G6

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 CCN et approuvée par le Conseil canadien des normes (CCN) conformément aux documents du CCN intitulés Exigences et lignes directrices – *Accréditation des organismes d'élaboration de normes et Exigences et lignes directrices – Approbation et désignation des Normes nationales du Canada*. On trouvera des renseignements supplémentaires sur les exigences relatives aux Normes nationales du Canada à l'adresse : www.ccn.ca. Une norme approuvée par le CCN est l'expression du consensus de différents experts dont les intérêts collectifs forment, autant que faire se peut, une représentation équilibrée des intéressés concernés. Les Normes nationales du Canada visent à apporter une contribution appréciable et opportune au bien du pays.

Le CCN est une société d'État qui fait partie du portefeuille d'Industrie Canada. 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. De plus, 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.

Comme les Normes nationales du Canada sont revues périodiquement, il est conseillé aux utilisateurs de toujours se procurer l'édition la plus récente de ces documents auprès de l'organisme d'élaboration de normes responsable de leur publication.

La responsabilité d'approuver les normes comme NNC incombe au :

Conseil canadien des normes
55, rue Metcalfe, bureau 600
Ottawa (Ontario) K1P 6L5 CANADA

Comment commander des publications de l'ONGC :

par téléphone	— 819-956-0425 ou — 1-800-665-2472
par télécopieur	— 819-956-5740
par la poste	— Centre des ventes de l'ONGC Gatineau, Canada K1A 1G6
en personne	— Place du Portage Phase III, 6B1 11, rue Laurier Gatineau (Québec)
par courrier électronique	— ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca
sur le Web	— www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html

NORME NATIONALE DU CANADA **CAN/CGSB-72.34-2017**

Remplace CAN/CGSB-72.34-2005

Enregistrements électroniques utilisés à titre de preuves documentaires

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

ICS 37.080

Publiée, mars 2017, par
l'Office des normes générales du Canada
Gatineau, Canada K1A 1G6

OFFICE DES NORMES GÉNÉRALES DU CANADA

Comité de gestion des documents et images électroniques

(Membres votants à la date d'approbation)

Présidente (Votant)

Duranti, L.	Interpares Trust (Intérêt général)

Catégorie d'intérêt général

Fox, U.	Arma Canada
Groulx, K.	The Advocates Society
Lachance, M.	Mindshare Consulting Services
Spiteri, L.	Dalhousie University

Catégorie producteur

Caughell, T.	Open Text Corporation
Davis, R.G.	Data Repro Com Limited
Knight, S.	Access Systems Ltd.
Krishnamoorthy, R.	Deloitte LLP
Knoppers, J. V.	Information Management Services (Infoman) Inc.
Priest, G.	Iron Mountain
Peterson, V.	CriticalControl SolutionsS

Catégorie organisme de réglementation

Cooper, R.	Secrétariat du Conseil du trésor
Jahn, C.	Agence des services frontaliers du Canada
Tremblay, G.	Agence du revenu du Canada

Catégorie utilisateur

Banks, T.	Services publics et Approvisionnement Canada
Ball, J.	Gendarmerie royale du Canada
Curley, D.	Bureau du Conseil privé
Earle, H.	Agriculture et Agroalimentaire Canada
Gourlie, M.	Association of Canadian Archivists
Laferrière, H.	Data Management Association (DAMA)
Meldrum, A.	Innovation, Sciences et Développement économique Canada
Stephens, S.	Association des banquiers canadiens

Secrétaire (non-votant)

Lozano, A.	Office des normes générales du Canada

Nous remercions Brian Thurgood et Lois Evans d'avoir dirigé le groupe de travail lors de la révision de la présente norme.

Nous remercions le Bureau de la traduction de Services publics et Approvisionnement Canada de la traduction de la présente Norme nationale du Canada.

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 audio-visuels, textes, fichiers multimédia, etc.) pour en favoriser l'admissibilité (voir 3.5 et 3.6) et le poids ou la valeur probante (voir 3.74) dans le cadre d'une procédure judiciaire. 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.

Cette norme s'harmonise aux lois fédérales, provinciales et territoriales et avec 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.

0 Introduction

0.1 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 intelligibles à 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 usagers, syntaxe, plateforme 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.

0.2 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* renferme la disposition suivante qui encourage l'utilisation de normes :

31.5 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.

0.3 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.

0.4 Termes et définitions

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

0.5 La version anglaise et la version 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 » [sauf dans les citations d'articles de loi où le mot « record » a été rendu par « pièce » en français]. 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 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 :

a) un cadre de procédures qui appuie des pratiques de qualité en matière de gestion des enregistrements;

b) 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 dans le 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 adresses 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 Source

Les publications susmentionnées peuvent être obtenues auprès du ministère de la Justice Canada, Direction des communications, Division des affaires publiques, 284, rue Wellington, Ottawa (Ontario) K1A 0H8, téléphone 613-957-4222, télécopieur 613-954-0811, 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.

3.1
accès
droit, possibilité ou moyen de trouver, de consulter ou d'extraire l'**information enregistrée**.

3.2
contrôle de l'accès
processus qui consiste à n'accorder qu'aux seules personnes autorisées l'**accès** aux **enregistrements** dans le **système d'enregistrements**.

3.3
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.

3.4
exactitude
mesure dans laquelle l'**information enregistrée** est précise, conforme, vraie, libre d'erreur ou de distorsion.

3.5
admissibilité (d'un enregistrement)
capacité de l'**information enregistrée** d'être produite en **preuve** dans une procédure judiciaire.

3.6
admissibilité (règles d'admissibilité)
règles en vertu desquelles les **enregistrements** sont jugés acceptables à titre de **preuves** dans une procédure judiciaire.

3.7
enregistrement analogue
enregistrement écrit sur du matériel physique comme du papier, un parchemin, une pierre, de l'argile, un film ou certains types de supports magnétiques audio et vidéo.

Voir aussi 3.51, enregistrement.

3.8
audit
examen systématique des activités permettant de veiller à ce que l'**information enregistrée** soit conforme aux politiques, **procédures** et contrôles sont établies et mises en œuvre de façon à ce que toutes les obligations financières, opérationnelles, juridiques et réglementaires soient satisfaites.

3.9
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.

3.10
enregistrement authentique
enregistrement qui est ce qu'il est censé être et n'a pas été altéré ou corrompu.

3.11
authentification
déclaration de l'**authenticité** à un moment particulier.

3.12
authenticité
qualité d'une entité qui est ce qu'elle est censée être et n'a pas été altérée ou corrompue.

3.13
personne autorisée
personne à qui une responsabilité précise a été confiée par une autorité supérieure qui a le pouvoir de le faire.

3.14
sauvegarde (copie)
Copie exacte des systèmes électroniques, des données et des programmes actifs faite à des fins de reprise en cas de panne du système ou de catastrophe.

3.15
saisie
enregistrement ou sauvegarde d'une instance en particulier d'une **information enregistrée**.

3.16
informatique en nuage
modèle qui permet d'accéder par réseau, en tout lieu et en tout temps, à un bassin partagé de ressources informatiques configurables qui peut être rapidement activé et désactivé et qui ne demande qu'un minimum d'effort de gestion ou d'interaction avec un fournisseur.

3.17
conversion
processus de transformation de l'**information enregistrée** d'un format à un autre.

Voir aussi 3.42, migration.

3.18
copie
double de l'**information enregistrée**.

3.19
donnée
plus petite unité significative d'**information enregistrée**.

3.20
destruction (des enregistrements)
processus qui consiste à éliminer des **enregistrements** de façon à ce qu'il soit impossible de les reconstituer.

3.21
numérique
représentation d'un objet ou d'un processus physique par des valeurs binaires discrètes.

3.22
numérisation
processus qui consiste à transposer sur un support électronique (numérique) une **information enregistrée** sur un support analogue.

Voir aussi 3.7, enregistrement analogue.

3.23
image disque
reproduction bit par bit du **support** de mise en mémoire et de son contenu, y compris les **données** ambiantes, l'espace de permutation et l'espace inutilisé.

3.24
disposition (des enregistrements)
mesure prise au sujet des **enregistrements** après l'expiration de leur **période de conservation,** c'est-à-dire **destruction, transfert** ou **préservation**.

3.25
document
unité indivisible d'**information enregistrée** qui présente un contenu stable et une forme fixe.

3.26
preuve documentaire
information enregistrée admise en **preuve** dans une procédure judiciaire.

3.27
communication de la preuve en format électronique (communication électronique)
procédure préalable au procès qui nécessite un échange d'enregistrements électroniques pertinents entre les parties.

3.28
information électronique
toute information enregistrée transmise par un conducteur électrique qui nécessite de passer par un équipement électronique pour être intelligible à une personne.

3.29
enregistrement électronique
enregistrement analogue ou numérique transmis par un conducteur électrique qui nécessite de passer par un équipement électronique pour être intelligible à une personne.

Voir aussi 3.51, enregistrement et 3.7, enregistrement analogue.

3.30
chiffrement
conversion de l'**information enregistrée** en un code secret (ou d'un texte en clair en texte chiffré).

3.31
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.

3.32
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.

3.33
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.

3.34
information
message destiné à des fins de communication.

3.35
sécurité de l'information
discipline multidisciplinaire 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).

3.36
système de la 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.

3.37
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.

3.38
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.

3.39
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.

3.40
support
support matériel sur lequel l'**information enregistrée** est mise en mémoire.

3.41
métadonnées
données servant à définir un **enregistrement** et à en décrire l'utilisation, la gestion, l'historique de conservation et les changements technologiques.

3.42
migration
processus qui consiste à transférer l'**information enregistrée** d'une configuration de **système de la TI** à une autre.

Voir aussi 3.17, conversion.

3.43
enregistrement officiel
instance d'un **enregistrement** qui a valeur d'**enregistrement original** final, complet et faisant autorité**.**

3.44
organisation
entité susceptible d'avoir des droits et des obligations prévus par la loi.

3.45
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.

3.46
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.

3.47
valeur probante
poids ou crédibilité accordée à une **preuve**.

Voir aussi 3.74, poids.

3.48
procédure
ensemble de règles, écrites ou non, qui régissent la conduite d'une transaction, ou les étapes formelles à franchir pour réaliser une transaction.

3.49
processus
séries de mesures, ou d'activités en général, exécutées pour franchir chaque étape formelle d'une **procédure**.

3.50
assurance de la qualité (enregistrements)
procédures permettant de surveiller et d'évaluer le **système d'enregistrement** dont l'objet est de maintenir un niveau de qualité souhaité.

3.51
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.

3.52
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**.

3.53
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**.

3.54
information enregistrée
information mise en mémoire sur un **support** de manière stable.

3.55
tenue des enregistrements
saisie, mise en mémoire, utilisation, tenue à jour et disposition des **enregistrements** et de leurs **métadonnées**.

3.56
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.

3.57
disposition d'un enregistrement
dernière mesure prise au sujet d'un enregistrement après l'expiration de sa période de conservation prescrite.

3.58
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 ou réception; classification; tenue à jour et utilisation; évaluation; **disposition** par **destruction** ou transfert à une institution ou à un service d'archivage; description dans les moteurs de recherche archivistiques; **préservation**; et référence et utilisation.

3.59
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**.

3.60
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**.

3.61
système de gestion des enregistrements
processus structuré, reposant sur les principes de la gestion des enregistrements, qui permet de contrôler la gestion des enregistrements associés à l'activité d'une organisation.

3.62
système de conservation des enregistrements
système électronique qui sert à conserver les **enregistrements électroniques** au fil des diverses générations technologiques.

3.63
période de conservation des enregistrements
période donnée pendant laquelle les **enregistrements** sont conservés pour répondre à des exigences opérationnelles, juridiques, réglementaires, financières ou autres.

3.64
système d'enregistrements
totalité des **enregistrements** d'une organisation et les systèmes de **gestion des enregistrements** et de préservation des **enregistrements** qui les contrôlent.

3.65
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.

3.66
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.

3.67
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.

3.68
enregistrement source; enregistrement original (numérisation)
enregistrement **analogue** à partir duquel une **copie** électronique (numérique) est faite.

Voir aussi 3.7, enregistrement analogue.

3.69
défaut de produire une preuve
destruction, falsification ou dissimulation de preuve.

3.70
transfert (enregistrements)
fait de confier le contrôle matériel, juridique et intellectuel des **enregistrements** à une autre organisation.

3.71
enregistrement temporaire
enregistrement qui n'a pas besoin d'être conservé pour répondre à des exigences opérationnelles, juridiques, réglementaires, financières ou autres.

3.72
enregistrement crédible
enregistrement exact, fiable et authentique.

3.73
système crédible
système d'enregistrements fiable et intègre.

3.74
poids (de la **preuve**)
crédibilité ou **valeur probante** d'une **preuve.**

4 Sigles et abréviations

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

AE Agent préposé aux enregistrements

AVEC Apportez votre équipement personnel de communication

COBO Informatique d'entreprise, opérations uniquement

COPE Informatique d'entreprise habilitée par l'utilisateur

EAT Examen assisté par la technologie

EDI Échange de données informatisées

FSIN Fournisseur de services d'informatique en nuage

GE Gestion des enregistrements

LPC Loi sur la preuve au Canada

TI Technologie de l'information

UPN Utilisez votre propre nuage

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

5.1 Généralités

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 [le mot « pièce » est utilisé dans la *LPC* au sens du mot « enregistrement »]. On trouve des dispositions comparables dans les lois des provinces et territoires qui s'appliquent aux procédures judiciaires assujetties aux lois de ces administrations.

Un système d'enregistrements peut comprendre :

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 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.*

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 fédéral, provinciaux et territoriaux permettent le remplacement de documents sources imprimés, ou de leurs copies, par des documents 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.

Le principe premier avancé par la présente norme est qu'une organisation doit toujours être en mesure de produire ses enregistrements en preuve. 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.

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). 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 la fiabilité du système (p. ex., paragraphe 31.3(a) de la *LPC*); ou

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

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 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 3.33). Il y a une exception à la règle du ouï-dire pour les enregistrements commerciaux (appelés aussi pièces commerciales), 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 ordinaire des affaires » de l'organisation dont provient l'enregistrement (p. ex. l'article 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, soit en vue d'un profit, soit à d'autres fins » (paragraphe 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 d'une organisation :

a) sources : l'origine des données figurant dans les enregistrements électroniques 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 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 est tenu des changements et modifications dans le système;

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 (section 6.4) et dans le guide de gestion du système de la TI (section 6.5).

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. 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 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. De plus en plus souvent, la communication électronique nécessite l'examen de milliers d'enregistrements pour en déterminer la pertinence et le caractère confidentiel. Ce genre d'examen se fait de plus en plus souvent à l'aide d'outils d'apprentissage automatique (examen assisté par la technologie ou EAT). 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 documents électroniques pertinents exigés par le tribunal afin que ces documents puissent être admissibles à titre de preuve dans les procédures judiciaires.

Pour en savoir plus, pour une investigation informatique dans les litiges civils, voir *Les principes de Sedona Canada*[1] et pour divulgation dans les procédures du droit pénal, voir R. v. Oler, 2014 CPAB 130 (CanLII).

5.3.1 Examen assisté par la technologie (EAT) 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 pas toujours du même avis au sujet de la précision de ces dispositifs. Pour obtenir des renseignements sur la façon de mener une découverte électronique à l'aide d'un EAT, voir *Les principes de Sedona Cana*da.

[1] *Les principes de Sedona Canada : L'administration de la preuve électronique* est l'un des projets du groupe de travail 7 (Sedona Canada) de la série *The Sedona Conference Working Group Series*. 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 l'adresse http://goo.gl/woLSFh

5.4 Mise en suspens pour des raisons juridiques

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 ». L'obligation de préserver l'information enregistrée s'applique dès qu'une poursuite est envisagée ou qu'une partie menace de l'intenter. 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 sera transmis à toutes les parties touchées, y compris les intervenants autres que les parties qui jouent un rôle pertinent et son propre personnel TI et de gestion des enregistrements. Cet avis devrait donner des instructions claires et détaillées sur les genres d'information à préserver. Il conviendra de le réémettre régulièrement et d'informer les gardiens des enregistrements du moment où ces exigences en matière de préservation sont levées.

Le système d'enregistrements sera capable de 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, produira par écrit et mettra en application une procédure de mise en suspens pour des raisons juridiques qui définira notamment les éléments suivants :

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 prévoira 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 indiquera 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.

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 la responsabilité de chaque personne au sein de l'organisation.

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 – 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 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,

---

[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 *Celanese Canada Inc. c. Murray Demolition Corp.,* 2006 CSC 36 [2006] 2 RCS 189.

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

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 sera 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 seront documentées dans le document d'authentification (p. ex., un affidavit).

6 Programme de gestion des enregistrements (GE)

6.1 Généralités

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 appuiera un système d'enregistrements réunissant des procédures et contrôles d'enregistrement appropriés qui viennent compléter les procédures opérationnelles d'affaires. L'organisation devra :

a) mettre sur pied un programme de GE;

b) adopter une politique de GE accompagnée de définition 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 vérifications 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

6.2.1 Autorisation

L'organisation autorisera, au moyen d'un instrument formel (p. ex., politique, directive, décret, règlement), 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 renverra aux pouvoirs et responsabilités confiés à l'organisation par la loi en ce qui concerne le programme de GE; confirmera 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 définira 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 et préservation);

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

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 sera clairement défini dans l'instrument formel d'autorisation de l'organisation (p. ex., politique, directive). L'organisation indiquera 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 service de l'extérieur). Si une partie ou la totalité du programme est délégué, les rôles et responsabilités du tiers autorisé seront clairement précisés et documentés, afin que la crédibilité des enregistrements électroniques ne soit pas compromise.

6.2.2.2 Fournisseur de services de l'extérieur

Quand une organisation a recours à un fournisseur de services contractuel pour la totalité ou une partie de son programme de GE, le fournisseur de services de l'extérieur se conformera à la politique et aux procédures du programme de GE et une disposition le stipulant se retrouvera dans tout document contractuel ou norme de service.

6.2.2.3 Recours à un fournisseur de services de l'extérieur

Dans le contrat conclu avec le fournisseur de services, la description détaillée des procédures, des processus et des pratiques englobera tous genres de services, y compris la gestion des installations, l'entreposage, 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 de l'extérieur se conforme à la politique, aux procédures, aux processus et aux pratiques de l'organisation. L'organisation conservera une copie de la preuve de conformité du fournisseur de services de l'extérieur et de l'efficacité et de la sécurité des services, ou aura accès à une telle preuve.

L'organisation n'aura recours à un fournisseur de services de l'extérieur qu'après avoir veillé à ce que le fournisseur en question 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.

6.2.2.4 Modifications au programme

Toute modification ou révision au programme de GE devra être approuvée par l'organisation.

6.3 Politique

6.3.1 Obligation d'avoir une politique

L'organisation aura 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

La politique de GE renfermera des dispositions pour :

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 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 de 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 de 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 et à la préservation des enregistrements;

g) faire en sorte 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

La conformité à la politique nécessite les éléments suivants :

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

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

c) le recensement des normes nationales ou internationales 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 toutes les directives, lois et règlements applicables.

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

6.4 Manuel de GE

6.4.1 Généralités

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

Le manuel de GE décrira 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 de GE sera tenu à jour et reflétera 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 de GE définira 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 de GE comprendra 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 de GE stipulera que des procédures de contrôle documentées seront mises en place pour les deux genres de saisie et précisera des niveaux d'assurance de la qualité pour faire en sorte que les enregistrements saisis soient exacts et complets.

Lorsque des systèmes de gestion du flux de travail sont mis en place, les détails opérationnels et les procédures de contrôle des changements seront documentés dans le manuel de 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.

Les procédures d'enregistrement non textuel utilisées (p. ex., audio, images, vidéo et multimédia) seront documentées dans le manuel de GE au même titre que les procédures utilisées pour toute autre forme d'enregistrement.

Le manuel de GE définira 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 sera documentée dans la documentation du système ainsi que les procédures. Une procédure de contrôle des versions sera établie pour tous les enregistrements.

Un jeu complet de métadonnées, y compris toute information pertinente aux fins de la preuve concernant l'identité de chaque enregistrement, les règles opérationnelles associées à sa saisie, sa structure logique et les définitions intégrales de l'entité et des attributs (voir l'annexe B), sera saisi ou créé et tenu à jour dans le système d'enregistrements aussi longtemps que l'enregistrement existe et parfois plus longtemps. Un profil de métadonnées organisationnelles sera établi pour les enregistrements.

6.4.2.2 Numérisation

Tout processus de numérisation s'alignera soigneusement sur les besoins opérationnels et sera conçu pour pouvoir créer des enregistrements numériques substituts de qualité suffisamment élevée à partir d'enregistrements analogues avec un minimum de perte d'information, de sorte que les enregistrements numériques substituts répondront aux besoins opérationnels courants tout comme aux exigences futures prévues. Le manuel de GE renfermera une liste des enregistrements analogues anciens et courants dont la numérisation est approuvée par l'organisation et documentera les motifs juridiques et opérationnels justifiant la destruction autorisée de tout enregistrement source. La renumérisation d'enregistrements initialement numériques sera évitée en raison des pertes inhérentes de qualité des enregistrements et de productivité opérationnelle.

Le manuel de GE exposera les procédures et les processus courants autorisés de numérisation pour assurer des reproductions exactes et lisibles des enregistrements sources sans altération du contenu ou de l'apparence, de même que des métadonnées appropriées aux fins de la gestion et de l'extraction des enregistrements. Au

minimum, des contrôles de qualité seront établis au stade de la préparation des documents ainsi qu'au moment du balayage et de l'indexation et au stade du téléchargement en vrac. L'assurance de la qualité sera menée et certifiée par l'organisation et les enregistrements sources ne seront pas 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 et reprises n'auront pas été documentées, approuvées et soumises.

Quand c'est un fournisseur qui assure les services de numérisation, c'est lui qui se charge de l'assurance de la qualité comme prévu au contrat et fournira une certification de l'assurance pour tous les enregistrements numérisés. De la même façon, les préposés aux dispositifs de numérisation au sein de l'organisation recevront la formation nécessaire pour que soient respectées toutes les exigences en matière d'assurance de la qualité et indiqueront que les activités d'assurance de la qualité ont été menées à bien par une signature ou une autre forme d'identification (p. ex., étampe, marque, identifiant électronique).

Les organisations seront en mesure d'attester que les versions numériques des documents analogues sont complètes et exactes, et qu'elles peuvent donc fournir une preuve des activités auxquelles les enregistrements sources ont servi. Ces enregistrements numériques seront découvrables et accessibles pour les personnes qui ont le droit d'y avoir accès, et ce, aussi longtemps que nécessaire.

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 (voir annexe B). Les éléments suivants devront être clairement indiqués dans le manuel de 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 supervisera et coordonnera toutes les activités associées qui permettent de s'assurer que les enregistrements dans le système d'enregistrements demeurent authentiques, accessibles et sécurisés.

L'AE tiendra à jour un registre des autorisations d'extraire, de lire, d'annoter, de modifier, de transmettre et de supprimer des enregistrements dans le système d'enregistrements (en d'autres termes, les privilèges d'accès) qui sont accordées aux agents et aux employés de l'organisation. L'AE s'assurera 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 (voir l'annexe B) 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 sera 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 seront 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) sera 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, 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 établie la valeur de chaque ensemble (classe ou catégorie) d'enregistrements, 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 veillera 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 sera 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 définira 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, transfert ou préservation. 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 de GE stipulera 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 de GE stipulera 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 sera 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 conservera en permanence ce registre des mesures de disposition à titre de preuve.

Le manuel de 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 de GE stipulera 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 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 de GE stipulera que les enregistrements transférés à un gardien désigné et acceptés par lui (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.

6.4.6.5 Préservation des enregistrements

Le manuel de GE indiquera 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 (voir l'annexe B) 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 devra 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 seront protégés contre l'obsolescence des logiciels.

6.4.6.5.1 Conservation et migration des enregistrements

Le manuel de GE donnera des consignes sur la conversion et la migration. La conservation 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 déterminera 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. Mais quel que soit le format de préservation choisi, la conversion et la migration seront intégrées dans un processus opérationnel bien documenté qui s'inscrit dans l'exploitation régulière du système d'enregistrements.

Les organisations auront une politique de conversion et de migration et le manuel de GE exposera des procédures détaillées permettant de faire en sorte que la structure, le contenu, les métadonnées d'identité et de tenue de documents (voir l'annexe B) 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.

6.4.6.5.2 Formats de préservation

Le manuel de GE indiquera 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 format 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 (voir l'annexe C).

6.4.7 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 destruction 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 et des audits de l'extérieur 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 signalera 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.

6.5 Guide de gestion du système de la TI

6.5.1 Généralités

Tous les éléments importants de l'architecture logique et physique du système de la TI où sont conservés les enregistrements seront intégralement documentés dans le 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 sera 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 comprendra 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 murs coupe-feu, 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) documentation des changements au 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;

g) procédures pour contrôler l'utilisation du matériel et des logiciels de maintenance du système qui peuvent contourner les contrôles d'accès au système, ainsi qu'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.

6.5.2 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 figureront 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 stipulera 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 sera 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 comprendra 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 seront documentées.

Le guide de gestion du système de la TI stipulera 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 l'intégrité des fichiers de données n'a pas été compromise. Le manuel stipulera également 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.

6.5.3 Sécurité et protection

6.5.3.1 Politique et procédures de sécurité de la TI

L'organisation aura 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 seront mises en œuvre en conformité de la politique de sécurité de la TI de l'organisation et elles 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 se fera 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 des supports de mise en mémoire sera conforme aux normes nationales ou internationales pertinentes.

6.5.3.2 Clés de chiffrement et signatures électroniques sécurisées

Lorsqu'il s'impose d'assurer la sauvegarde de l'information enregistrée, un système de chiffrement sera 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 seront 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 seront valides, seront conservées en lieu sûr et seront mises à la disposition des personnes autorisées seulement.

6.5.3.3 Enregistrements électroniques évolutifs

Certains enregistrements électroniques peuvent contenir des codes automatiquement exécutables (qu'on appelle souvent des macros), qui peuvent modifier un fichier chaque fois qu'il est extrait, visualisé ou imprimé (p. ex., la date et l'heure courantes seront automatiquement insérées). L'existence de tels codes dans un fichier signifie que le fichier n'est pas figé. Chaque fois qu'il est ouvert, il pourra paraître différent, même si l'usager n'y a apporté aucune modification.

Dans le contexte de la valeur probante, cette fonction se rapporte directement au « cours usuel et ordinaire des affaires », qui tient compte du fait que les enregistrements d'une organisation changent. Il faut faire la différence entre les genres de changements selon qu'ils concernent le contenu de l'enregistrement, les métadonnées ou la forme documentaire. Pour veiller à ce qu'un enregistrement électronique puisse être utilisé en preuve dans le cadre d'une procédure judiciaire, les organisations doivent empêcher les modifications automatiques sous quelque forme que ce soit, afin que des copies authentiques puissent être fournies.

6.5.3.4 Horodatage

La vérification régulière des horloges des ordinateurs pour confirmer l'exactitude de la date et de l'heure sera 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 seront documentées.

L'organisation désignera 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.

6.5.4 Transmission des enregistrements

Les organisations veilleront à ce qu'il y ait interopérabilité parmi les technologies qu'elles utilisent et entre leurs propres technologies et celles d'autres organisations avec lesquelles elles interagissent dans le cours usuel et ordinaire des affaires. Lorsque des enregistrements sont transmis entre des systèmes informatiques, des applications ou des supports de mise en mémoire, l'intégrité des enregistrements sera vérifiée régulièrement au moyen d'une procédure de vérification.

6.5.5 Piste de vérification

6.5.5.1 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 seront saisies continuellement et qu'elles seront toujours protégées contre l'altération et la perte. Les données d'audit sont enregistrées dans une piste de vérification.

Les pistes de vérification renfermeront 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 se composera 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 seront documentées dans le guide de gestion du système de la TI.

6.5.5.2 Gestion des enregistrements constituant la piste de vérification

Les registres de piste de vérification seront assujettis à des procédures de gestion interne des enregistrements semblables à celles qui régissent d'autres enregistrements essentiels de l'organisation et figureront à titre de type de document spécifique dans le guide de gestion du système de la TI. Des dispositions seront 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 seront conservées.

6.5.5.3 Contenu de la piste de vérification

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

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

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

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

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

iii) création, modification ou suppression de métadonnées;

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

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

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

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

6.5.5.4 Création de la piste de vérification

Les données de la piste de vérification seront générées automatiquement par le système de la TI. Si elles ne le sont pas, les procédures pour générer les données piste de vérification seront documentées dans le guide de gestion du système de la TI et elles s'appliqueront à l'organisation et à tout fournisseur de service contractuel de l'extérieur.

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

6.5.5.5 Accès

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

6.5.5.6 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 seront documentés dans la piste de vérification. Les procédures de migration ou de conversion comprendront des méthodes démontrant que toutes métadonnées connexes sont elles aussi transférées ou converties et seront 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 seront documentés dans le registre de la piste de vérification.

6.5.5.7 Flux de travail

S'il existe des systèmes de flux de travail, le guide de gestion du système de la TI établira 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.

6.5.5.8 Vérification

Les données de la piste de vérification seront 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.

7 Nouvelles technologies

Il arrive de plus en plus souvent que les organisations créent, gèrent et utilisent des enregistrements dans une variété d'environnements, de services et de dispositifs sur Internet. Leurs avantages et leurs risques seront recensés dans le cadre d'un processus d'évaluation des risques.

7.1 Évaluation des risques

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

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 déterminer les tribunes de participation;

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 de GE et du guide de gestion du système de la TI);

g) établir un processus de prise de décisions au sujet des propositions actuelles et futures se rapportant à la nouvelle technologie;

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

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. Les incidences juridiques complexes des nouvelles technologies seront soigneusement examinées au moyen d'une approche multidisciplinaire (p. ex., aspects juridiques, sécurité, protection des renseignements personnels, TI, gestion des risques, etc.) qui tient compte de l'infrastructure existante et de la tolérance aux risques de l'organisation.

7.2 Informatique en nuage

7.2.1 Administration compétente

Lorsqu'elle a recours à l'informatique en nuage, l'organisation déterminera dans quelle administration ses données/ses enregistrements seront conservés. Il arrive fréquemment qu'un fournisseur de services d'informatique en nuage (FSIN) ait des centres de données dans plus d'un pays. En outre, comme le matériel numérique est continuellement déplacé d'un serveur à un autre selon l'espace disponible et pour la sécurité assurée par la dispersion géographique, il est pratiquement impossible d'établir où il se trouve à tel ou tel moment. Au Canada, il est interdit que l'information enregistrée détenue par des organismes publics au sujet des citoyens canadiens, de même que toute voie de transmission et de sauvegarde des données, soit conservée à l'extérieur des limites géographiques du pays, et

c'est aux organismes publics qu'il incombera de se conformer à cette règle. Par conséquent, les organismes publics le détermineront avant d'envisager une solution d'informatique en nuage; les organismes privés doivent également tenir compte des questions territoriales.

7.2.2 Protection des renseignements personnels

La protection des renseignements personnels est un autre enjeu de premier plan que soulève l'informatique en nuage. Même si l'information enregistrée est conservée physiquement à l'intérieur des frontières géographiques du Canada, l'accès en ligne signifie qu'elle peut être accessible de n'importe où, ou encore piratée, falsifiée ou sortie de son contexte. De plus, rien ne garantit que les enregistrements dont la destruction est prévue seront bel et bien détruits dans tous les endroits où ils existent, car des copies de redondance ou de sauvegarde peuvent exister. Dans de nombreux cas, les liens donnant accès à l'information sont supprimés, mais le matériel lui-même n'est pas détruit. Compte tenu des exigences de la législation canadienne entourant les renseignements personnels, ces problèmes d'accès et la permanence involontaire des enregistrements entraînent un passif important associé à l'informatique en nuage.

Les organisations veilleront à ce qu'il soit stipulé dans leur entente contractuelle avec le FSIN qu'elles doivent être informées immédiatement de toute violation de l'accès et que leurs exigences en matière de conservation et de disposition seront respectées, le fournisseur démontrant que les enregistrements sont protégés, préservés et détruits selon les directives. L'entente avec le fournisseur stipulera 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.

Les organisations incluront dans l'entente avec leur FSIN des dispositions relatives à la mise en mémoire des enregistrements concernant les ex-employés et la responsabilité par rapport à ces enregistrements.

7.2.3 Règles d'admissibilité

Les enregistrements conservés dans un environnement infonuagique devront continuer de satisfaire aux règles d'admissibilité. L'AE, avec le soutien de la TI, établira un moyen d'authentifier les enregistrements conservés dans le nuage et déterminera quelle instance d'un même enregistrement constitue l'enregistrement officiel de l'organisation. La création, la tenue à jour et l'utilisation de l'enregistrement dans l'environnement infonuagique seront documentées (voir annexe D).

7.2.4 Intégration des systèmes d'enregistrements

Étant donné que toutes les organisations ont des enregistrements pour lesquels ils ne peuvent risquer l'accès non autorisé ou la perte d'accès (p. ex. enregistrements confidentiels), les organisations qui choisissent l'informatique en nuage pour ces enregistrements doivent maintenir un système d'enregistrements hybride et de tels enregistrements demeureront dans l'infrastructure interne. L'organisation veillera à ce que les exigences de programme soient respectées, peu importe que les enregistrements soient conservés par un ou plusieurs fournisseurs de services d'informatique en nuage ou dans un système interne.

7.3 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 partant 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 se doteront d'une politique sur les médias sociaux qui définira le moment à partir duquel une publication est considérée comme un enregistrement. Elles définiront 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 seront mis en mémoire par l'organisme 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 (voir annexe E).

7.4 Appareils mobiles

Les organisations permettront peut-être à leurs employés d'utiliser leurs propres appareils pour s'acquitter de leurs fonctions lorsqu'il semble que les avantages sont supérieurs aux risques. Le concept AVEC/UPN présente un certain nombre de défis en matière de licences de bases de données et de logiciels, de sécurité, de protection des renseignements personnels, de propriété intellectuelle et de loi sur l'emploi, car l'utilisation des appareils ne connaît pas de frontière (voir annexe F).

Après avoir mené une évaluation des risques, l'organisation diffusera une politique clairement définie et strictement applicable. La politique doit indiquer clairement si elle prend en charge le AVEC (en gérant tous les enregistrements créés sur des appareils personnels ou seulement les enregistrements créés sur de tels appareils par un segment de l'organisation), si elle permet le AVEC sans le prendre en charge (p. ex. chaque employé est responsable de la gestion des enregistrements de l'organisation dans l'appareil ou de leur transfert dans le système de tenue des dossiers de l'organisation) ou si elle ne le permet pas. Dans ce dernier cas, la politique doit indiquer si elle permet les appareils COBO (Informatique d'entreprise, opérations seulement) ou COPE (Informatique d'entreprise habilitée par l'utilisateur) ou si elle permet à chaque employé de choisir l'une des trois options. Pour chacun des cas, la politique doit comprendre des détails tels que les types d'appareils utilisés, le partage des coûts entre l'employeur et l'employé, les droits d'accès, les modalités de soutien, le suivi et la surveillance, la destruction des données à distance, les activités interdites, l'interdiction d'utilisation par toute autre personne que l'employé et les obligations réciproques à la cessation d'emploi.

Les procédures de gestion des enregistrements utilisant les appareils personnels ou le propre nuage des employés seront intégrées au manuel de GE; les procédures de gestion des appareils seront intégrées au guide de gestion du système de la TI.

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'accompagnement (au niveau fédéral, provincial et territorial).

b) Les exigences et normes en matière de technologie, information et 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 a 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.

Annexe B
(informative)

Métadonnées

B.1 La production, la gestion, la disposition et la préservation des métadonnées devraient être formellement autorisées par l'organisation dans le manuel de GE.

B.1.1 Le manuel de GE 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 et à authentifier l'enregistrement et à donner accès à l'enregistrement.

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

c) 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).

d) font partie intégrale de l'enregistrement. D'autres métadonnées s'accumulent pendant le cycle de vie de l'enregistrement et leur production et leur gestion font partie intégrante du système d'enregistrements.

e) permettent aux usagers de comprendre et d'interpréter l'enregistrement.

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

B.1.2 Les métadonnées peuvent être classifiées selon le moment où elles ont été produites et leur objet. Les métadonnées produites au moment de la création d'un enregistrement pour identifier celui-ci sont des *métadonnées d'identité* et peuvent comprendre :

a) des métadonnées temporelles – qui précisent la date à laquelle l'enregistrement est produit ou reçu ou mis en mémoire dans un regroupement d'enregistrements;

b) des métadonnées concernant des personnes – qui précisent le nom de l'auteur ou des auteurs de l'enregistrement, du ou des destinataires et d'autres personnes qui l'ont reçu ainsi que du bureau *de prise en charge,* s'il y a lieu;

c) des métadonnées concernant la forme – qui précisent la forme documentaire que revêt l'enregistrement (p. ex., lettre, note de service) et la nature de son contenu (p. ex., contrat, sentence, brevet, candidature);

d) des métadonnées techniques – qui précisent le format et d'autres caractéristiques technologiques de l'enregistrement;

e) des métadonnées de dénomination – qui précisent le nom de l'enregistrement, son objet ou l'action qu'il englobe;

f) des métadonnées de relations – qui précisent les relations entre l'enregistrement et d'autres enregistrements (p. ex., numéro dans un registre, code de classification, numéro d'identification);

g) des métadonnées d'authentification – qui précisent la méthode d'identification de l'enregistrement s'il y a lieu (p. ex., sceau numérique, signature numérique, chiffrement).

B.1.3 Les métadonnées d'identité, qui sont partie intégrante de l'enregistrement à la création, doivent être conservées avec l'enregistrement aussi longtemps que celui-ci existe, autrement l'enregistrement perdra son intégrité.

B.1.4 Certaines métadonnées sont ajoutées tout au long du cycle de vie de l'enregistrement pour attester de changements techniques ou de changements dans la forme, d'ajouts, de transferts d'un endroit à un autre ou de la cession de la responsabilité de l'enregistrement, ou pour permettre la mise en œuvre de procédures et de processus de gestion des enregistrements, y compris l'accès et l'extraction, les restrictions d'accès, la conservation et la disposition. Il s'agit des métadonnées de tenue de documents et elles rentrent dans les catégories suivantes :

a) Métadonnées descriptives – qui sont utilisées pour trouver et interpréter l'enregistrement.

b) Métadonnées administratives – qui sont utilisées pour gérer l'enregistrement et peuvent comprendre les suivantes :

   i) métadonnées techniques – qui fournissent de l'information sur le contexte technique de l'enregistrement, la migration vers un nouveau système et les méthodes de disposition;

   ii) métadonnées sur les droits – qui décrivent les droits et les obligations concernant l'enregistrement, y compris la propriété, les droits d'auteur et d'autres droits de propriété intellectuelle, les restrictions d'usage et de sécurité;

   iii) métadonnées de préservation – qui décrivent les activités qui ont eu lieu pour préserver l'enregistrement au fil du temps et au fil des changements technologiques, par exemple conversion et reproduction à des fins de redondance.

   iv) Métadonnées structurelles – qui documentent les relations structurelles entre des enregistrements numériques ou à l'intérieur d'enregistrements numériques (p. ex., les hyperliens qui renvoient à différentes pages d'un site Web).

   v) Métadonnées d'utilisation – au sujet des usagers de la ressource ou qui proviennent de ces usagers (p. ex., étiquettes sociales, registre d'accès, registre des recherches faites par les usagers).

B.1.5 Les métadonnées de tenue de documents ne font pas partie de l'identité de l'enregistrement, mais comme elles sont générées dans le cours de la tenue à jour et de l'utilisation de l'enregistrement, elles révèlent les actions dans le cadre desquelles l'enregistrement a servi, ainsi que le cours usuel et ordinaire des affaires. Les métadonnées peuvent être détruites quand elles sont remplacées par d'autres métadonnées, mais seulement si cette action s'inscrit dans la façon usuelle et ordinaire dont le créateur gère ses enregistrements. L'organisation ne doit pas oublier que les métadonnées peuvent inclure des renseignements personnels et, par conséquent, être visées par les lois sur la protection des renseignements personnels.

Annexe C
(informative)

Formats de préservation

L'analyse qui suit est présentée à titre illustratif seulement et n'a pas pour objet de recommander un format en particulier – la norme professe l'agnosticisme en matière de technologie – mais plutôt de faire état de certaines questions à prendre en considération au moment de choisir un format de préservation (p. ex., un format ouvert qui est généralement reconnu).

Au niveau des enregistrements textuels, un format de fichier est conçu expressément pour la préservation à long terme des enregistrements. Le format de document portable (PDF), ISO 32000-1:2008, est un format de fichier propre à la livraison de documents sous forme de pages sans égard à la plateforme et il préserve l'apparence du document lorsqu'il est visualisé à partir de multiples architectures. Toutefois, si l'affichage précis de la police de caractères est une exigence en matière de preuve, le format PDF/A, ISO 19005-1:2005 sera privilégié. Même s'il n'accepte pas de contenu audio/vidéo ni JavaScript et qu'il ne permet ni compression ni chiffrement, le format PDF/A nécessite que toutes les polices de caractères soient intégrées et applique les règles de métadonnées de la plateforme Extensible Metadata Platform (XMP) d'Adobe tout en offrant la possibilité de fournir de nouveaux schémas de métadonnées au besoin. Le format PDF/A-2, ISO 19005-2:2011 et ISO 32000-1, offrait une accessibilité accrue, et notamment des améliorations pour les fichiers de plus petite taille, permettait le recours à la compression d'images en format JPEG2000 et pouvait prendre en charge d'autres fichiers PDF/A en pièces jointes. Le format PDF/A-3, ISO 19005-3:2012, présente les mêmes fonctionnalités que le PDF/A-2, mais en plus d'autres fichiers PDF/A, il peut intégrer n'importe quel type de flux de données. Les visualiseurs de documents conçus en fonction de cette spécification afficheront le contenu de l'enregistrement comme dans le format PDF/A-2, mais peuvent présenter une fonctionnalité supplémentaire recommandée qui fait qu'à la demande des usagers, les données intégrées peuvent être extraites du PDF et utilisées/ouvertes de toute manière voulue.

Du point de vue de la conversion des enregistrements et de la migration des documents, que ce soit pour régler des problèmes d'obsolescence ou tout simplement pour améliorer la lisibilité ou la convivialité sur diverses plateformes, il semble que le format PDF/A-3 pourrait répondre aux exigences en matière de preuve pour les enregistrements commerciaux aussi bien que dans la perspective de la meilleure preuve. Même si les éléments visuels statiques du principal document visualisé présentent le contenu de l'enregistrement de manière fixe, un ou plusieurs jeux de métadonnées contextuelles peuvent être conservés dans les sections des données passives pour en assurer l'authenticité. On peut répondre à toute préoccupation concernant la meilleure preuve ou l'intégrité en intégrant le flux binaire original de l'enregistrement source lui-même.

Annexe D
(informative)

Informatique en nuage

D.1 Par « informatique en nuage », on entend l'utilisation d'une vaste gamme d'infrastructures et de services distribués sur un réseau (généralement Internet), évolutifs sur demande (lorsque les capacités peuvent être augmentées et réduites de façon élastique), et conçus pour prendre en charge le stockage et la gestion de grands volumes de matériel numérique. Les caractéristiques essentielles de l'informatique en nuage sont les suivantes : libre-service sur demande, accès global au réseau, mise en commun des ressources, élasticité rapide et tarification à l'utilisation.

Les modèles de service les plus courants sont les suivants : le logiciel comme service (Software as a Service ou SaaS), la plateforme comme service (Platform as a Service ou PaaS) et l'infrastructure comme service (Infrastructure as a Service ou IaaS). Les fournisseurs de services d'informatique en nuage (FSIN) offrent un certain nombre de modèles de déploiement, notamment le nuage privé, le nuage communautaire, le nuage public et le nuage hybride. Il est important de ne pas confondre informatique en nuage et entreposage des enregistrements de l'organisation sur Internet dans un lieu qui relève du contrôle de l'organisation.

La norme de fiabilité des services d'informatique en nuage offerts par un FSIN de l'extérieur est la même que pour toute autre transaction dans le marché : *caveat emptor,* c'est-à-dire que l'acheteur prenne garde. Les organisations qui ont recours à des services d'informatique en nuage dispensés par un FSIN de l'extérieur se placent volontairement en position de vulnérabilité et de dépendance, compte tenu de l'évaluation des risques; chaque organisation devrait peser les avantages et les risques de recourir à l'informatique en nuage.

D.1.1 L'informatique en nuage présente divers avantages :

a) Réduction des coûts : L'avantage le plus évident, car l'organisation n'a pas besoin de posséder le matériel/les logiciels réseau en propre et peut éviter des coûts d'investissements importants. De plus, certains coûts liés au personnel de la TI pourront être moindres; les coûts de l'énergie seront réduits; il n'y aura pas de coûts de mise à niveau de technologie, car le système d'utilisation partagée permet de mettre en commun des ressources pour en obtenir plus à moindre coût; et les coûts seront limités, car l'organisation ne paiera que les services qu'elle utilise.

b) Évolutivité : La fourniture des services est flexible et peut être augmentée ou réduite au besoin.

c) Disponibilité : Les services sont accessibles sur demande, en tout temps et en tout lieu, à condition d'avoir accès au réseau.

d) Sécurité : Les fournisseurs de services d'informatique en nuage peuvent miser sur une masse critique pour offrir des technologies et un contrôle centralisé plus complexes et plus coûteux que ce qu'une organisation pourrait s'offrir seule.

e) Collaboration : Les usagers, qu'ils soient dans la même région ou dans des régions différentes, peuvent systématiquement accéder à du matériel qui est continuellement mis à jour et mis à disposition à partir d'une source centrale et partager le matériel.

D.1.2 Ces avantages s'accompagnent de risques. Les organisations devraient faire une évaluation des risques de l'adoption de l'informatique en nuage, compte tenu de différents facteurs :

a) Coût : Les coûts de l'informatique en nuage demeurent élevés. Le transfert des ressources d'information existantes, l'établissement de nouveaux processus opérationnels, la mise en œuvre de contrôles et le chiffrement et les frais à la demande peuvent être plus élevés que prévu. Les coûts peuvent afficher une grande variabilité dans les organisations en raison de changements dans les tendances d'utilisation et de coûts inattendus comme les hausses des droits de licence.

b) Évolutivité : Les organisations auront peut-être de la difficulté à estimer leurs besoins en matière de services et à en faire le suivi.

c) Disponibilité : Les organisations dépendent du FSIN pour assurer la continuité des services et des affaires.

d) Fiabilité : Il peut arriver que les FSIN perdent des ressources d'information à cause de procédures de traitement ou de sauvegarde défectueuses. Un FSIN peut être racheté, déclarer faillite ou autrement disparaître sans préavis suffisant.

e) Portabilité et interopérabilité : Les organisations auront peut-être de la difficulté à transférer des actifs numériques entre fournisseurs ou entre services.

f) Sécurité : L'accès non autorisé par des FSIN, des sous-traitants ou des pirates et les menaces internes présentent les risques les plus importants pour la sécurité des actifs numériques détenus ou en transit, de même que la gestion inefficace de l'accès. La cohabitation pose le risque que des actifs numériques soient regroupés avec ceux d'une autre organisation. Les interfaces de programmes d'application n'auront peut-être pas les caractéristiques de sécurité nécessaires. La surveillance des contrôles de sécurité peut être insuffisante ou les contrôles peuvent être ignorés.

g) Modalités du service : Il se peut que les attentes de l'organisation ne soient pas satisfaites par un contrat standard avec le FSIN, particulièrement en ce qui concerne la production et la propriété des métadonnées, les exigences en matière de protection des renseignements personnels, la conformité et les besoins en matière d'audit.

h) Contrôles : Il se peut que les organisations éprouvent de la difficulté à prouver la légitimité de leur système de tenue de documents et d'un enregistrement particulier requis en preuve. Il faut des contrôles significatifs pour prouver l'authenticité (c'est-à-dire l'identité et l'intégrité) des enregistrements, et les organisations disposent de moins de contrôle en ce sens lorsqu'elles ont recours à l'informatique en nuage.

i) Transparence : Il se peut que les organisations constatent après coup que le FSIN ne fournit pas suffisamment d'information ou n'assure pas un accès suffisant pour répondre aux exigences concernant les enregistrements à titre de preuve.

D.2 Comme il peut être plus difficile de démontrer les processus de création, de tenue à jour et d'utilisation ainsi que la chaîne de possession des enregistrements conservés dans le nuage par rapport aux enregistrements conservés à l'interne, la nature des enregistrements commerciaux dans le nuage peut être plus facilement remise en question du fait que le matériel conservé dans le nuage peut être piraté et falsifié. Cela signifie également que l'intégrité des enregistrements dans le nuage ne peut pas être démontrée au moyen d'une analyse inforensique, en ce sens que leur tenue à jour, leur traitement et leur préservation ne sont pas répétables, vérifiables ou objectifs, comme le stipulent les processus d'authentification inforensique et qu'en conséquence, ils ne peuvent pas être utilisés à titre de preuve. L'intégrité de reproduction des enregistrements dans le nuage n'est pas non plus démontrable (c'est-à-dire qu'il est impossible de démontrer que le processus de création d'un double n'a pas altéré intentionnellement ou accidentellement l'original et que le double est une copie bit par bit exacte de l'original). Ce type d'intégrité est extrêmement important pour la préservation, parce que la seule façon de préserver des enregistrements numériques est de les reproduire, de sorte que les processus de reproduction et de migration doivent essentiellement être transparents pour que les enregistrements puissent être dignes de confiance. Les méthodes utilisées pour recueillir et analyser des enregistrements numériques et les méthodes utilisées pour les acquérir et les préserver ne devraient pas modifier les entités numériques, ou si elles les modifient, ces changements devraient être repérables. L'admissibilité des enregistrements tenus dans le nuage est possible si le contrat avec le FSC prévoit l'accès aux métadonnées liées à l'identité et à la tenue des enregistrements (voir annexe C) ainsi que la capacité de vérifier l'intégrité du système.

Annexe E
(informative)

Médias sociaux

Les médias sociaux sont des applications et des services conçus pour faciliter la collaboration par la création et l'échange de contenus créés par les usagers. Ils comprennent les blogues/microblogues, les wikis, les flux RSS, le partage multimédia, le partage de signets/l'étiquetage social, les services de réseautage social, les applications composites (« mashups »), les mondes virtuels et les outils de révision en collaboration. Les applications de médias sociaux utilisent le Web comme plateforme, permettent de partager le contenu généré par les usagers, souvent recueilli par externalisation, et bâtissent des réseaux reposant sur une architecture de participation et d'ouverture. Le contenu produit par les applications de médias sociaux est souvent offert en preuve, mais il peut être difficile à saisir, à préserver et à authentifier.

Comme l'informatique en nuage, les médias sociaux posent de nombreux défis, notamment atteintes à la vie privée, violations de la confidentialité, diffamation, violations de droits d'auteur et de marques de commerce, usage personnel impropre (par opposition à un usage acceptable par l'organisation), violations des droits de la personne (affichages discriminatoires), griefs dans le milieu de travail (intimidation et harcèlement au travail) et conformité avec des décisions des tribunaux (ne pas afficher les noms de personnes en cause dans un procès frappé d'une interdiction de publication).

Quoi qu'il en soit, les gouvernements ont recours aux médias sociaux pour offrir des services à la clientèle, faciliter l'accès à l'information, diffuser des avis en situation d'urgence et proposer des occasions de participation communautaire. Ce faisant, ils créent des enregistrements publics, particulièrement lorsque le public est appelé à participer à la prise de décisions et à des consultations sur des politiques, mais également lorsque les employés collaborent au moyen d'outils comme le GCpédia (le Wikipédia du gouvernement du Canada). À l'heure actuelle, les applications de médias sociaux les plus couramment utilisées par les gouvernements comprennent Facebook, Twitter et YouTube.

Les organisations de tous genres ont recours aux médias sociaux comme le font les gouvernements, mais plus intensément à des fins de relations publiques et pour effectuer des transactions, de sorte que les enregistrements électroniques qu'elles créent dans le cadre de ces processus soulèvent des préoccupations particulières lorsqu'il s'agit de les utiliser en preuve.

La caractéristique principale des enregistrements créés dans les médias sociaux est leur caractère éphémère apparent, qui s'oppose à leur pérennité dans les faits. D'un côté, la nature dynamique de ces sites rend difficile la récupération des enregistrements quand on en a besoin, mais d'un autre côté, l'absence de contrôle par l'usager ne garantit pas que les enregistrements seront supprimés quand c'est souhaité ou requis.

Une autre caractéristique importante des enregistrements créés dans les médias sociaux est l'absence de contexte stable et l'existence de multiples contextes possibles, qui peuvent donner différentes significations aux enregistrements. Dans le contexte d'un gazouillis, par exemple, le contexte est-il la page sur laquelle le gazouillis apparaît, ou les gazouillis précédents et suivants du même auteur? Est-ce l'événement auquel le message se rapporte ou le moment particulier où il a été affiché?

De plus, a) les plateformes de médias sociaux facilitent la transmission du matériel d'un cercle de personnes à un autre et les lignes de démarcation entre le public et le privé peuvent ainsi s'estomper; b) les contributions attribuées ou liées à des comptes dans les médias sociaux de personnes maintenant décédées ou des programmes, des comités ou des organismes qui n'existent plus c) des groupes dynamiques ad hoc d'employés créent collectivement des corpus de matériel interrelié concernant un projet de travail ou un intérêt commun, de sorte qu'on peut se demander qui est le propriétaire ou l'auteur du matériel; et d) la pratique de la réutilisation donne souvent lieu à un *remixage*, qui donne lui-même lieu à des produits imités qui transforment substantiellement l'intention et le contexte du matériel initial. De nouvelles normes sociales font leur apparition au fil des cycles successifs d'utilisation, de réutilisation, de modification, de reconversion et d'avis de suppression.

Annexe F
(informative)

Appareils mobiles

AVEC signifie « Apportez votre équipement personnel de communication », c'est-à-dire la tendance émergente chez les employés d'une organisation à utiliser leurs propres portables, tablettes, mini-portatifs (« netbooks »), téléphones intelligents ou d'autres appareils mobiles pour leur travail. Cette pratique a et continuera d'avoir des incidences significatives sur la sécurité des technologies de l'information au cours des prochaines années.

UPN signifie « Utilisez votre propre nuage », c'est-à-dire la tendance émergente pour les employés de recourir à des services d'informatique en nuage de tiers du secteur privé ou du secteur public pour conserver les enregistrements de l'organisation pour laquelle ils travaillent. Les pratiques UPN et AVEC sont inextricablement liées, car lorsque les enregistrements d'une organisation sont conservés dans des dispositifs portatifs personnels, il faut passer par Internet pour y avoir accès.

Cette tendance mondiale, appelée consumérisation de la TI, ou COTI, est le fait des employés qui achètent leurs propres appareils pour effectuer le travail de leur organisation, utilisent leurs propres comptes de services personnels en ligne, installent leurs propres applications puis se branchent au réseau de l'organisation à partir de leur appareil, souvent sans que l'organisation soit au courant ou qu'elle ait donné son accord.

Les pratiques AVEC et UPN soulèvent de grandes préoccupations, semblables à celles qui sont soulevées par l'informatique en nuage et les médias sociaux : à qui appartiennent les enregistrements? Qui y a accès? L'employé peut-il compartimenter les enregistrements utilisés pour le travail, afin que l'organisation puisse y avoir accès mais que les renseignements personnels de l'employé sur l'appareil puissent être protégés? Les données sur l'appareil répondent-elles à la définition juridique d'« enregistrement »? Sont-elles accessibles pour utilisation? Les enregistrements sur l'appareil sont-ils admissibles à titre de preuves documentaires ou de preuves matérielles dans le cadre d'une procédure judiciaire? L'organisation peut-elle être protégée contre le vol ou la perte de l'appareil, les intrusions, la diffamation par le propriétaire de l'appareil, les atteintes à la vie privée? Suivant le cycle de vie de l'enregistrement, de quelle façon l'organisation peut-elle avoir accès à l'information opérationnelle qui se trouve sur l'appareil de l'employé, l'utiliser, la protéger et la préserver?

Les organisations ont recours à des processus décisionnels complexes pour protéger leurs systèmes et l'information de nature délicate et pour assurer une sécurité raisonnable et justifiable face à la loi. Elles investissent dans des contrôles techniques, administratifs et matériels reflétés dans des politiques de sécurité documentées qu'elles déterminent comme étant suffisants pour réduire les risques à la sécurité à un niveau acceptable.

Les organisations éprouveront de la difficulté à atténuer les risques pour la sécurité si elles ne contrôlent pas la conformité à leurs propres protocoles de sécurité. Elles devraient exiger le chiffrement à des fins de sécurité de toute l'information de nature délicate sur les appareils dont elles sont propriétaires. Il pourrait être difficile d'appliquer ces mêmes normes aux appareils mobiles des employés. Si l'appareil d'un employé est piraté ou volé et que l'information non chiffrée est récupérée, la sécurité des appareils mobiles de l'organisation sera vraisemblablement le premier domaine à être examiné à la loupe.

En même temps, les organisations devraient examiner les avantages et les risques des pratiques AVEC/UPN. Certaines organisations ont déjà accepté ces pratiques à l'issue d'un tel examen.

Avantages perçus de la pratique AVEC :

a) Réduction des coûts : Réduction, voire élimination, des investissements des organisations dans des appareils mobiles ou d'autres dispositifs informatiques pour équiper les employés afin qu'ils s'acquittent de leur travail au quotidien.

b) Productivité améliorée : Les employés tendent à passer plus de temps à utiliser leurs propres appareils, auxquels ils ont accès 24 heures par jour. Il est possible que cette accessibilité se traduise par une augmentation de la productivité.

c) Efficience : Il est fort probable que les appareils des employés soient plus à jour que ceux de l'organisation, ce qui peut se traduire par une plus grande efficience.

Toutefois, la pratique AVEC représente de gros défis au chapitre des interventions en cas d'incident et des investigations qui ont des incidences sur la fiabilité, l'exactitude et l'authenticité des enregistrements, ainsi que sur les renseignements personnels des employés et la confidentialité et la sécurité de l'organisation. S'il doit y avoir une enquête, il peut être difficile d'obtenir l'accès à l'appareil ou sa possession. C'est particulièrement le cas quand c'est l'employé lui-même qui est visé par l'enquête. S'il faut recueillir et préserver la preuve documentaire conservée dans un appareil personnel, l'incapacité d'y avoir accès et de prendre possession de l'appareil peut avoir des conséquences extrêmement préjudiciables. Si une organisation n'est pas en mesure de conserver et de protéger des enregistrements qui pourraient servir en preuve dans un litige, elle pourrait s'exposer à des sanctions.

Beaucoup d'organisations commencent à élargir l'éventail des outils qu'elles utilisent au-delà des téléphones intelligents et des tablettes et à accepter les pratiques AVEC pour les PC ainsi que les Ultrabooks et les mini-PC présentant une empreinte réduite. Il est probable que les employeurs découvrent de nouvelles façons d'utiliser les appareils émergents qui n'avaient pas été comprises à l'origine par les planificateurs de la TI, comme dans le cas de l'iPad. Les organisations plus tolérantes aux risques voudront peut-être laisser leurs employés utiliser les nouveaux dispositifs et en tirer des enseignements, pour évaluer les avantages de ces nouveaux appareils.

La tendance ne s'arrêtera pas aux pratiques « prenez votre propre PC » et « utilisez votre propre nuage », et la tendance « utilisez votre propre TI » est imminente. Ces nouveaux outils encourageront rapidement les employés à utiliser leurs propres applications, leurs propres systèmes et peut-être même leurs propres réseaux sociaux au travail.

Les possibilités à exploiter sont indéniables, mais on s'attend à ce que des événements émergents obligent les organisations qui ont tardé à adopter ces pratiques à faire preuve de prudence. Il pourrait s'agir par exemple de reportages faisant état de fuites de données importantes à partir de l'appareil d'un employé et de préoccupations de la part d'employés et de syndicats au sujet des incidences de l'accès en tout temps, en tout lieu – est-ce que ça signifie que l'employé est tenu de répondre en tout temps, en tout lieu? Les renseignements personnels et le lieu où se trouve l'employé pourraient être visibles à l'employeur, ce qui pourrait empiéter sur la vie privée de l'employé.

Les organisations les premières à adopter ces pratiques et qui veulent « obliger » les employés à prendre leurs appareils personnels se heurteront peut-être à de l'opposition si les employés estiment que c'est une mesure d'économie à leurs dépens. Toutefois, les coûts cachés de la transition d'un système efficace de soutien de la TI vers un mécanisme d'autosuffisance de la part des employés pourront gruger toutes les économies découlant de la pratique AVEC. Cette question demeurera à l'avant-plan pendant encore un certain temps chez les planificateurs de la TI, même si des politiques « blindées » sont adoptées en matière de AVEC.

Les organisations devraient procéder à des évaluations exhaustives des risques associés à la pratique AVEC portant notamment sur les éléments suivants :

a) Sécurité : La probabilité d'accès non autorisé à des renseignements de nature délicate par des parties de l'intérieur comme de l'extérieur est élevée, de sorte que la sécurité devrait être serrée.

b) Redondance : La probabilité que des renseignements essentiels soient conservés uniquement sur ces appareils plutôt que sur les serveurs sécurisés de l'organisation nécessite que de multiples copies des enregistrements soient faites, au cas où l'appareil serait perdu, détruit ou inaccessible à un moment critique.

c) Susceptibilité de faire l'objet d'un audit : les organisations qui traitent ou qui manipulent des données confidentielles sont souvent auditées ou exigent des audits de leurs systèmes et processus de sécurité. Il serait difficile d'obtenir les autorisations de sécurité requises dans un environnement où les appareils personnels sont utilisés, parce que l'audit des enregistrements conservés dans des appareils personnels pourrait constituer une violation de la vie privée de l'employé, de sorte qu'il serait impossible de mener des audits exhaustifs. Il faudra adopter des procédures explicites.

d) Propriété des données : Dans un environnement où les appareils personnels sont utilisés, la propriété des enregistrements peut poser problème et il faudra déterminer clairement les enregistrements conservés dans un appareil personnel qui appartiennent légitimement à l'organisation.

e) Chaîne de possession : Les organisations n'exerceront plus de contrôle sur les enregistrements conservés dans les appareils personnels de leurs employés; elles doivent donc réglementer la façon dont ces enregistrements sont produits ou reçus ou mis en mémoire, la façon dont ils peuvent être utilisés par d'autres employés, la façon dont des copies en sont faites et contrôlées et la façon dont les enregistrements sont transférés aux serveurs de l'organisation pour pouvoir être régis par les procédures de GE de l'organisation, comme la classification, la conservation et la disposition, et la façon dont ils seront intégrés au système d'enregistrements.

f) Information nécessaire à la gestion : Les organisations ne disposeront pas immédiatement ni systématiquement des enregistrements nécessaires pour prendre des décisions de gestion clés, de sorte qu'elles devront établir quels enregistrements ont besoin d'être transférés ou copiés rapidement à partir des appareils personnels ou quels enregistrements devraient être disponibles à l'époque en cause à partir du nuage de l'organisation.

g) Conservation et mise en suspens pour des raisons juridiques : Il faut vérifier constamment que les enregistrements désignés pour conservation à long terme sont protégés; une mise en suspens pour des raisons juridiques doit également pouvoir être imposée sur les enregistrements dans les appareils personnels dès que c'est nécessaire.

h) Disposition des ressources informationnelles : Il arrive souvent que les employés ne fassent pas attention à la suppression des enregistrements qui doivent être éliminés. Il est essentiel d'établir comment les enregistrements sur les appareils personnels seront détruits en toute sécurité sans pouvoir être récupérés, conformément au calendrier de conservation et de disposition de l'organisation.

i) Intégrité des données : Il est hautement improbable que l'intégrité des enregistrements puisse être maintenue, ni même vérifiée, dans un environnement où des appareils personnels sont utilisés, et c'est la principale raison pour laquelle des procédures strictes au sujet du transfert des enregistrements au serveur ou au nuage de l'organisation s'imposent.

j) Cessation d'emploi : Lorsqu'un employé est remercié de ses services ou quitte l'organisation, il est presque certain qu'il emportera délibérément ou par erreur des enregistrements conservés dans ses appareils personnels, de sorte que l'organisation a besoin d'une procédure claire pour éviter que cela se produise dans la mesure du possible.

k) Perte de revenus : Les organisations risquent de perdre des revenus lorsqu'elles ne disposent pas de tous les enregistrements nécessaires à des fins de facturation. Il peut aussi arriver que des employés utilisent des enregistrements conservés dans leurs appareils personnels pour aller se chercher un revenu clandestin. Il faut des règlements pour éviter que cela se produise.

Deux étapes additionnelles peuvent être suivies pour réduire les risques associés à AVEC et UPN sont le déploiement d'une solution de gestion des appareils mobiles ou de gestion de mobilité d'entreprise et l'utilisation d'un client léger – où une application accède à l'information traitée et stockée dans les serveurs de l'organisation.

Les solutions de rechange valides à AVEC sont la COBO, où les organisations possèdent les appareils utilisés par les employés et ne permettent pas leur utilisation à des fins personnelles, et la COPE, où les organisations possèdent les appareils utilisés par les employés, mais dont les appareils sont configurés pour permettre leur utilisation dans le cadre d'activités personnelles. Il est possible pour une organisation de mélanger les stratégies en fonction de sa structure et de son uniformité. Si certaines parties de l'organisation ont des exigences uniques ou des profils de sécurité particuliers, l'organisation voudra peut-être prendre en charge plusieurs solutions en même temps plutôt que de choisir une solution unique.

Bibliographie

[1] American National Standards Institute (ANSI). ANSI/ARMA 18-2011 *Implications of Web-based, Collaborative Technologies in Records Management.* Disponible auprès de: IHS Markit. www.global.ihs.com/

[2] American National Standards Institute (ANSI). ANSI/ARMA 19-2012 *Policy Design for Managing Electronic Messages.* Disponible auprès de: IHS Markit. www.global.ihs.com/

[3] ARMA International. TR 24-2013, *Best Practices for Managing Electronic Messages.* Disponible auprès de: IHS Markit. www.global.ihs.com/

[4] ARMA International. *Guideline for Outsourcing Records Storage to the Cloud* (2010). Disponible auprès de: IHS Markit. www.global.ihs.com/

[5] Office des normes générales du Canada (ONGC). CAN/CGSB-72.11, *Microfilms et images électroniques — Preuve documentaire.* Disponible auprès de: Office des normes générales du Canada, Centre des ventes, Gatineau, Canada K1A 1G6. Téléphone 819-956-0425 ou 1-800-665-2472. Télécopieur 819-956-5740. Courriel ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca. Site Web www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-fra.html.

[6] Association canadienne de normalisation (CSA). CAN/CSA-ISO/IEC 11179-3-13, *Information technology — Metadata registries (MDR) — Part 3: registry metamodel and basic attributes.* Disponible auprès de: http://shop.csa.ca/

[7] Association canadienne de normalisation (CSA). CAN/CSA-ISO/IEC 14662-01, *Technologie de l'information — Modèle de référence EDI-ouvert.* Disponible auprès de: http://shop.csa.ca/

[8] Organisation internationale de normalisation (ISO). ISO/TR 13028 *Information et documentation – Mise en oeuvre des lignes directrices pour la numérisation des enregistrements.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[9] Organisation internationale de normalisation (ISO). ISO 15489-1 *Information et documentation — « Records management » — Partie 1: Principes directeurs.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[10] Organisation internationale de normalisation (ISO). ISO/TR 15489-2 *Information et documentation — « Records management » — Partie 2: Guide pratique.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[11] Organisation internationale de normalisation (ISO). ISO 15801 *Images électroniques – Stockage électronique d'informations — Recommandations pour les informations de valeur et leur fiabilité.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[12 Organisation internationale de normalisation (ISO). ISO 19005 *Document management –Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).* Disponible auprès de : IHS Markit. www.global.ihs.com/

[13] Organisation internationale de normalisation (ISO). ISO 19005 *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).* Disponible auprès de : IHS Markit. www.global.ihs.com/

[14] Organisation internationale de normalisation (ISO). ISO 19005 *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).* Disponible auprès de : IHS Markit. www.global.ihs.com/

[15] Organisation internationale de normalisation (ISO). ISO/IEC 27001 *Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences*. Disponible auprès de : IHS Markit. www.global.ihs.com/

[16] Organisation internationale de normalisation (ISO). ISO/IEC 27002 *Technologies de l'information -- Techniques de sécurité -- Code de bonne pratique pour le management de la sécurité de l'information.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[17] Organisation internationale de normalisation (ISO). ISO/IEC 27005 *Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information.* Disponible auprès de : IHS Markit. www.global.ihs.com/

[18] Sedona Canada. The Sedona Conference Working Group 7 (2015), *Les principes de Sedona Canada sur l'administration de la preuve électronique (deuxième édition)*.