



LIGNES DIRECTRICES POUR LA GESTION DES COURRIELS

FEUILLE DE ROUTE

BIBLIOTHÈQUE ET ARCHIVES CANADA

Direction des documents gouvernementaux

2008



Bibliothèque et Archives Canada
Library and Archives Canada

Canada



Table des matières

0. Introduction aux lignes directrices pour la gestion des courriels	1
0.1. Références	1
0.2. Lignes directrices	3
0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde?	3
0.4. Quels sont les résultats attendus?	4
0.5. Pourquoi la gestion des courriels est-elle si importante?	5
0.6. Domaines où les lignes directrices ne s'appliquent pas	6
0.7. Feuille de route pour se conformer aux lignes directrices.....	6
0.8. Cycle de vie de l'information électronique	7
0.9. Définitions.....	9
1. Les institutions doivent se doter d'un plan pour gérer les courriels	17
1.1. Gérer les programmes et les systèmes de courriel de manière intégrée	18
1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels	20
1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels	21
1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, ont été bien distribuées, lues et comprises.....	22
1.5. Conserver des dossiers sur les activités de formation et sur la participation.....	23
2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles.....	25
2.1. Créer, expédier et stocker les courriels de manière structurée	26
2.2. Recevoir et stocker les courriels de manière structurée	27
2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière.....	28
2.4. Garder un seul exemplaire de chaque courriel	30
2.5. Gérer et conserver les pièces jointes aux courriels.....	31
2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada	32
2.7. Utiliser avec modération les listes de diffusion institutionnelles	33
2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource	35
2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu.....	37
2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu.....	38
2.11. Éviter d'utiliser la fonction « Répondre à tous ».....	40
3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles	42



3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels.....	42
3.2. Déterminer où classer la copie « officielle »	44
3.3. Conserver les métadonnées associées aux courriels.....	44
3.4. Classifier et classer les courriels systématiquement et fréquemment.....	47
3.5. Gérer le stockage en ligne temporaire des courriels.....	48
3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels.....	49
3.7. Limiter le contenu des courriels à un seul sujet.....	52
3.8. Décrire l'objet d'un courriel en termes clairs et significatifs.....	53
3.9. Prévoir un système d'indexation des courriels	53
3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (<i>threading</i>)	55
4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels	56
4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur	57
4.2. Utiliser les journaux d'exploitation pour créer une piste de vérification et veiller au respect des règles	58
4.3. Afficher les noms dans les en-têtes et les adresses de courriel	59
4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique.....	61
4.5. Surveiller la performance des activités de découverte et de disposition des courriels	62
5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés	65
5.1. Éviter de procéder à des purges indiscriminées dans les systèmes de courriel	66
5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées	67
5.3. Enlever le chiffrement avant de quitter une institution	68
5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada.....	70
5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel.....	71
5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets	72
5.7. Protéger les systèmes contre les pertes ou les dommages	74
5.8. Employer le bon niveau de classification de sécurité.....	75
5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun.....	76
5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel.....	78
5.11. Utiliser des mesures de protection et d'authentification des messages	80



5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre	81
5.13. Utiliser la signature numérique s'il y a lieu.....	82
5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada	84
5.15. Ne pas employer de signature numérisée pour signer un courriel.....	85
5.16. Utiliser le chiffrement s'il y a lieu.....	86
5.17. Employer le stockage de proximité pour la conservation à long terme des courriels	88
5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore	89
5.19. Protéger les courriels en protégeant les supports de conservation	91
5.20. Protéger les courriels de l'obsolescence.....	92
5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel.....	93
5.22. Conserver en permanence la documentation du système de courriel.....	94
5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes	95
5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document	96
6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes	99
6.1. Obtenir une autorisation de disposition des courriels.....	99
6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun.....	100
6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP	102
7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin	104
7.1. Évaluer l'efficacité de la gestion des courriels	104
8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels	106
8.1. Responsabilités des utilisateurs	106
8.2. Responsabilités des administrateurs de réseaux ou de systèmes.....	108
8.3. Responsabilités des spécialistes en gestion de l'information	110
8.4. Responsabilités des gestionnaires des opérations.....	113
8.5. Responsabilités des dirigeants.....	115



Annexes

- ANNEXE A. RÔLES ET RESPONSABILITÉS**

- ANNEXE B. RESPECT DES LIGNES DIRECTRICES POUR LA GESTION DES COURRIELS ET
PLAN DE MISE EN OEUVRE**

- ANNEXE C. LOIS, RÈGLEMENTS, POLITIQUES ET ENTENTES QUI NÉCESSITENT
L'APPLICATION DES LIGNES DIRECTRICES POUR LA GESTION DES COURRIELS**

- ANNEXE D. TABLEAU DES NORMES TECHNIQUES ET PROCÉDURALES**



0. Introduction aux lignes directrices pour la gestion des courriels

0.1. Références

0.1.1 Nom : Lignes directrices pour la gestion des courriels

0.1.2 Catégorie : Lignes directrices

0.1.3 Autorisation : Bibliothèque et Archives Canada

0.1.4 Organisme responsable : Bibliothèque et Archives Canada

0.1.5 Index croisé

(Documents reliés au sujet: lois, politiques, directives et normes – Gouvernement du Canada, autres sources)

Correspondance entre les lois et politiques et le Cadre de la gestion de l'information				
Lois et politiques reliées au cycle de vie de l'information				
Lois et politiques	Création Saisie	Organisation Utilisation Diffusion	Tenue à jour et préservation	Disposition
Accès à l'information, Loi et règlements sur l'	X	X	X	X
Accès à l'information, Politique sur l'	X	X	X	X
Apprentissage, de formation et de perfectionnement, Politique en matière d'				
Autorisation et l'authentification électroniques, Politique sur l'			X	
Bibliothèque et les Archives du Canada, Loi sur la	X	X	X	X
Charte canadienne des droits et libertés		X		
Communication, Politique de	X	X	X	X
Droit d'auteur, Loi sur le			X	
Emploi dans la fonction publique, Loi sur l'		X		
Évaluation, Politique d'			X	
Évaluation des facteurs relatifs à la vie privée, Politique d'	X	X	X	X
Gestion de l'information, Politique sur la	X	X	X	X



Correspondance entre les lois et politiques et le Cadre de la gestion de l'information				
Lois et politiques reliées au cycle de vie de l'information				
Lois et politiques	Création Saisie	Organisation Utilisation Diffusion	Tenue à jour et préservation	Disposition
Gestion de l'information sur le personnel, Politique sur la	X	X		
Gestion de l'infrastructure à clé publique, Politique de			X	
Gestion des finances publiques, Loi sur la	X	X	X	
Gestion des projets, Politique sur la		X		
Gestion des risques, Politique sur la			X	
Gestion des technologies de l'information, Politique sur la	X		X	
Langues officielles, Loi sur les		X		
Preuve au Canada, Loi sur la	X	X	X	
Protection civile, Loi sur la			X	
Protection de l'information, Loi sur la			X	
Protection des renseignements personnels, Loi et règlements sur la	X	X	X	X
Protection des renseignements personnels, Politique sur la	X	X	X	
Protection des renseignements personnels et des documents électroniques, Loi sur la	X	X	X	X
Responsabilité civile de l'État et le contentieux administratif, Loi sur la			X	
Rôles et responsabilités en matière de gestion de l'information, Directive sur les	X	X	X	X
Sécurité, Politique sur la		X	X	
Service canadien du renseignement de sécurité, Loi sur le	X	X	X	
Services communs, Politique sur les	X	X		
Statistique, Loi sur la	X	X	X	
Utilisation des réseaux électroniques, Politique d'		X	X	
Vérificateur général, Loi sur le		X		

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg09_f.asp)



0.2. Lignes directrices

Vous êtes sur le point d'entreprendre la lecture d'un document contenant des lignes directrices relatives à la gestion des courriels dans l'ensemble du gouvernement canadien. Chacune de ces lignes directrices comporte une ou plusieurs recommandations afin de vous aider à obtenir les résultats attendus.

Ces lignes directrices et les recommandations associées ne sont pas obligatoires, mais elles se veulent une référence, un modèle d'excellence.

0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde?

En vertu de la Politique de gestion de l'information, les ministères et organismes (ci-après « les institutions ») du gouvernement fédéral doivent recueillir, créer, recevoir et saisir tous les documents relatifs à leurs activités organisationnelles, incluant les messages électroniques (courriels) qui contiennent de l'information faisant partie de la mémoire institutionnelle ou des données utilisées pour prendre une décision ou entreprendre une action. La Politique de gestion de l'information et la Directive sur les rôles et responsabilités en matière de gestion de l'information identifient des responsabilités précises pour tous les employés du gouvernement.

L'administrateur général est responsable devant son ministre et le Conseil du Trésor d'une gestion efficace et bien coordonnée de l'information pour l'ensemble de son ministère. Chaque employé du gouvernement, sans exception, a un rôle à jouer dans la gestion des courriels.

Pour donner de bons résultats, les Lignes directrices pour la gestion des courriels doivent s'intéresser aux interventions humaines autant qu'aux systèmes électroniques. En d'autres mots, les machines sont incapables de prendre toutes les décisions que suppose la gestion des courriels.

Les dirigeants trouveront, dans les présentes lignes directrices, des ressources pour les aider à intégrer les exigences de la gestion de l'information dans toutes les activités de conception, de mise en œuvre, d'évaluation et de rapport découlant des programmes et services de leur organisation.

Les spécialistes en technologies de l'information peuvent s'attendre à trouver dans ces lignes directrices des normes et des orientations relatives à la configuration et au fonctionnement des ordinateurs et des réseaux (équipements et logiciels) qui sous-tendent les courriels.

Les spécialistes en gestion de l'information trouveront ici des orientations concernant la gestion des courriels à toutes les étapes de leur cycle de vie: création ou réception, classement, stockage, récupération et disposition.



Le personnel professionnel, les contractuels et les autres utilisateurs de courriel trouveront dans ces lignes directrices et les recommandations associées des éléments d'orientation non techniques dont ils devront tenir compte chaque fois qu'ils utiliseront leur courriel.

Par conséquent, ces lignes directrices s'adressent à un très large public.

- Dirigeants
- Gestionnaires
- Professionnels en gestion de l'information (GI)
- Professionnels en technologie de l'information (TI)
- Utilisateurs du courriel

Ces personnes ont différents rôles à jouer, n'ayant pas toutes le même niveau de connaissance des activités organisationnelles, de compétence technique ou d'autorité. Certaines ont plus d'un rôle à jouer. Ainsi, le dirigeant et le professionnel en TI portent chacun deux chapeaux : l'un est un spécialiste des opérations, l'autre un expert en technologie, mais ce qu'ils ont en commun, et avec tous les autres employés de l'organisation, c'est qu'ils sont aussi des utilisateurs du courriel.

0.4. Quels sont les résultats attendus?

On reconnaît généralement qu'il est impossible de gérer les courriels selon un mode entièrement centralisé. Essentiellement, le processus de gestion du courriel commence avec les utilisateurs, qui doivent chaque jour, à leur écran d'ordinateur, décider quels messages éliminer et quels messages conserver, et où classer ces derniers.

Les lignes directrices et recommandations contenues dans le présent document proposent des procédures visant à garantir la conservation de la bonne information, au bon moment, et pour la bonne période de temps. Notez bien que ce document ne recommande pas de délai de conservation particulier pour les courriels. En effet, les délais de conservation varient selon le sujet ou la fonction du courriel et sont établis par chaque institution, conformément aux exigences légales et organisationnelles applicables à cette dernière.

Afin que les utilisateurs soient bien informés quant à la manière de gérer les courriels reçus et envoyés, les dirigeants et les gestionnaires auront droit à des recommandations supplémentaires très précises concernant la formation du personnel et son adhésion à ces lignes directrices.

Les procédures techniques décrites dans le présent document s'adressent aux spécialistes en technologie de l'information (TI) et en gestion de l'information (GI) qui participeront à la mise en place de l'infrastructure technologique appropriée.

Certaines des recommandations formulées dans ces lignes directrices s'adresseront spécifiquement à l'un ou l'autre des groupes mentionnés ci-dessus. D'autres recommandations s'appliqueront à plus d'un groupe. Dans ce cas, les groupes auront probablement des rôles



différents à jouer dans la mise en œuvre des lignes directrices; leurs rôles respectifs seront alors précisés.

0.5. Pourquoi la gestion des courriels est-elle si importante?

Tout simplement parce que le courriel est largement utilisé pour prendre des décisions, assigner des tâches, transmettre des rapports d'étape, confirmer des transactions, et à plusieurs autres fins reliées aux opérations du gouvernement. Les courriels relatifs aux activités gouvernementales sont des documents à part entière et, à ce titre, doivent être conservés durant une période de temps déterminée ou conservés en permanence, en vertu des politiques et législations en vigueur. Alors que certaines informations doivent être conservées pendant une période de temps minimale, d'autres sont assujetties à des délais de conservation maximaux, à l'expiration desquels elles doivent être éliminées, conformément à la loi.

On estime actuellement, qu'en moyenne, un employé du gouvernement reçoit ou crée au moins 50 courriels par jour, ce qui donne un total de 10 000 courriels par année pour 200 jours ouvrables. Dans le cas d'un ministère comptant 5 000 employés, cela représente plus de 50 millions de courriels par an. Le nombre total d'employés dans la fonction publique a dépassé 350 000 au cours des cinq dernières années; un simple calcul révèle que, dans l'ensemble, les employés du gouvernement pourraient traiter jusqu'à 3 milliards 500 millions de courriels par an. Ce volume de courriels exerce une pression importante sur la capacité de stockage des serveurs, en raison de la quantité de données contenues dans les courriels et les fichiers qui y sont joints. Plus important encore, les courriels sont à l'heure actuelle le principal canal de prise de décision au gouvernement et, pour des fins de reddition de compte, ces documents doivent être gérés avec soin et efficience, afin de garantir qu'ils soient classés et stockés de façon appropriée, et qu'ils puissent être récupérés au besoin, tout au long de leur période de conservation.

Bibliothèque et Archives Canada

Dans le but d'appuyer ses politiques, ses programmes et ses services, le gouvernement du Canada crée et gère chaque année des documents sur divers supports d'enregistrement, de plus en plus sous forme électronique. Ces documents, qui vont de la correspondance aux enregistrements audiovisuels et sonores, en passant par les énoncés de politiques, les ententes, les rapports de recherche, les dossiers opérationnels ou d'exploitation, les marchés, les actes notariés, les baux, les enquêtes et la prestation de services, les données statistiques, les photographies, les dessins architecturaux, les plans et les cartes, sont essentiels :

- à l'administration efficiente du gouvernement lorsqu'il fait des affaires et gère les affaires de l'État au nom des Canadiens;
- à la capacité des citoyens à tenir le gouvernement responsable de ses décisions et actions dans notre société démocratique;
- à la préservation de la connaissance de notre histoire nationale et de notre mémoire collective au profit des générations futures.

(Source : <http://www.collectionscanada.gc.ca/gestion-information/007/007007-1042-f.html>)



0.6. Domaines où les lignes directrices ne s'appliquent pas

Les listes et forums de discussion, ainsi que les listes et calendriers de diffusion constituent des éléments de la gestion des courriels qui ne sont pas abordés dans ces lignes directrices. Cela ne veut pas dire qu'ils ne sont pas importants ou qu'on ne devrait pas s'y intéresser à l'avenir, mais pour l'instant, ces sujets n'ont pas été traités dans la présente version des Lignes directrices pour la gestion des courriels - Feuille de route.

0.7. Feuille de route pour se conformer aux lignes directrices

Le document « Lignes directrices pour la gestion des courriels - Feuille de route » présente l'ensemble de lignes directrices, ainsi qu'une justification et des résultats à atteindre pour chacune d'elles. Chaque institution devra prendre en compte toutes les lignes directrices et recommandations associées; cependant, certaines de ces lignes directrices et recommandations pourront être interprétées à la lumière du mandat et des exigences organisationnelles propres à l'institution.

Par conséquent, chacune des lignes directrices et chacune des recommandations devra peut-être être appuyée par une décision et un énoncé de politique de la part de la haute direction de l'institution. La feuille de route a pour objectif de simplifier la rédaction d'une telle politique en proposant un modèle de politique pour chacune des lignes directrices et des actions recommandées. Le texte d'introduction à la politique de gestion des courriels de l'institution devrait indiquer clairement pourquoi l'institution a élaboré une telle politique, et quels seront les bénéfices attendus pour elle-même et ses employés. Vous trouverez ci-dessous un exemple d'introduction.

Introduction à la politique de gestion des courriels

Exemple d'énoncé de politique

(Nom de l'institution) a adopté la politique suivante concernant la gestion des courriels.

L'utilisation du courriel au gouvernement et dans l'entreprise privée a pris des proportions inattendues. Selon des estimations conservatrices, les employés du gouvernement du Canada reçoivent ou expédient plus de trois milliards de courriels par année, et ce nombre augmente régulièrement. Il n'est donc pas étonnant que le courriel constitue, à l'heure actuelle, l'un des plus importants défis en matière de gestion de l'information au gouvernement du Canada. Les courriels et leurs pièces jointes renferment souvent des informations relatives à une décision ou à une action. Ils peuvent aussi contenir un conseil, ou les termes d'une entente ou d'une transaction. Dans ces cas, les courriels seront probablement considérés comme des documents du gouvernement du Canada et, à ce titre, devront être conservés pendant une période de temps appropriée – et, pour certains, de façon permanente.



Les documents relatifs à des décisions, actions, ententes et transactions font partie de ceux qui doivent être conservés dans une société démocratique, ceci afin de garantir la responsabilisation du gouvernement à l'égard de ses citoyens. Puisque le courriel est maintenant aussi largement utilisé, les messages électroniques sont devenus une forme de preuve fréquemment exigée dans les actions en justice et les audits. Par conséquent, il est essentiel que les courriels soient correctement classifiés, classés et conservés, afin que l'on puisse les retrouver au besoin, et en démontrer hors de tout doute l'authenticité, l'intégrité et la fiabilité.

Les risques associés à une utilisation ou à une gestion inappropriées des courriels sont nombreux.

- Il peut être difficile et coûteux (ou même impossible) de retrouver des documents ou de l'information de première importance.
- Si des courriels doivent être produits en preuve, il peut être difficile d'en établir l'authenticité ou la fiabilité.
- Des messages à caractère non officiel peuvent être confondus avec des engagements officiels.
- Des courriels non protégés peuvent être divulgués à des personnes autres que le destinataire prévu.
- Il peut s'avérer difficile de trouver des documents qui doivent être éliminés en vertu d'une obligation légale.

Dans le but de relever ces défis, le gouvernement du Canada propose des lignes directrices pour la gestion des courriels, des métadonnées et des pièces jointes qui s'harmonisent avec les lois et politiques en vigueur et avec les autres normes et lignes directrices apparentées. Afin de tenir compte de leurs mandat, mission et contexte respectifs, les institutions peuvent procéder à une certaine interprétation des lignes directrices et recommandations associées, et offrir des conseils quant à leur mise en œuvre.

Le mandat de (nom de l'institution) est (indiquer le mandat).

La mission de (nom de l'institution) est (indiquer la mission).

L'information et les documents officiels communiqués par l'intermédiaire du courriel de (nom de l'institution) doivent être identifiés, gérés, protégés et conservés tant qu'ils sont nécessaires aux opérations courantes, aux audits, aux actions en justice, à la recherche ou à toute autre fin prévue.

Cette politique a pour but d'informer les employés à tous les niveaux de l'organisation, notamment les dirigeants, les spécialistes en gestion de l'information, les spécialistes en technologie de l'information (dont les administrateurs de réseaux), les gestionnaires et les utilisateurs (employés, contractuels et autres utilisateurs), de leurs rôles respectifs relativement à l'utilisation, à la gestion et à la conservation des courriels.

0.8. Cycle de vie de l'information électronique

Les recommandations contenues dans les présentes lignes directrices pour la gestion des courriels s'articulent autour des sept phases du cycle de vie de l'information électronique.

Planification

Cueillette, création, réception et saisie

Organisation

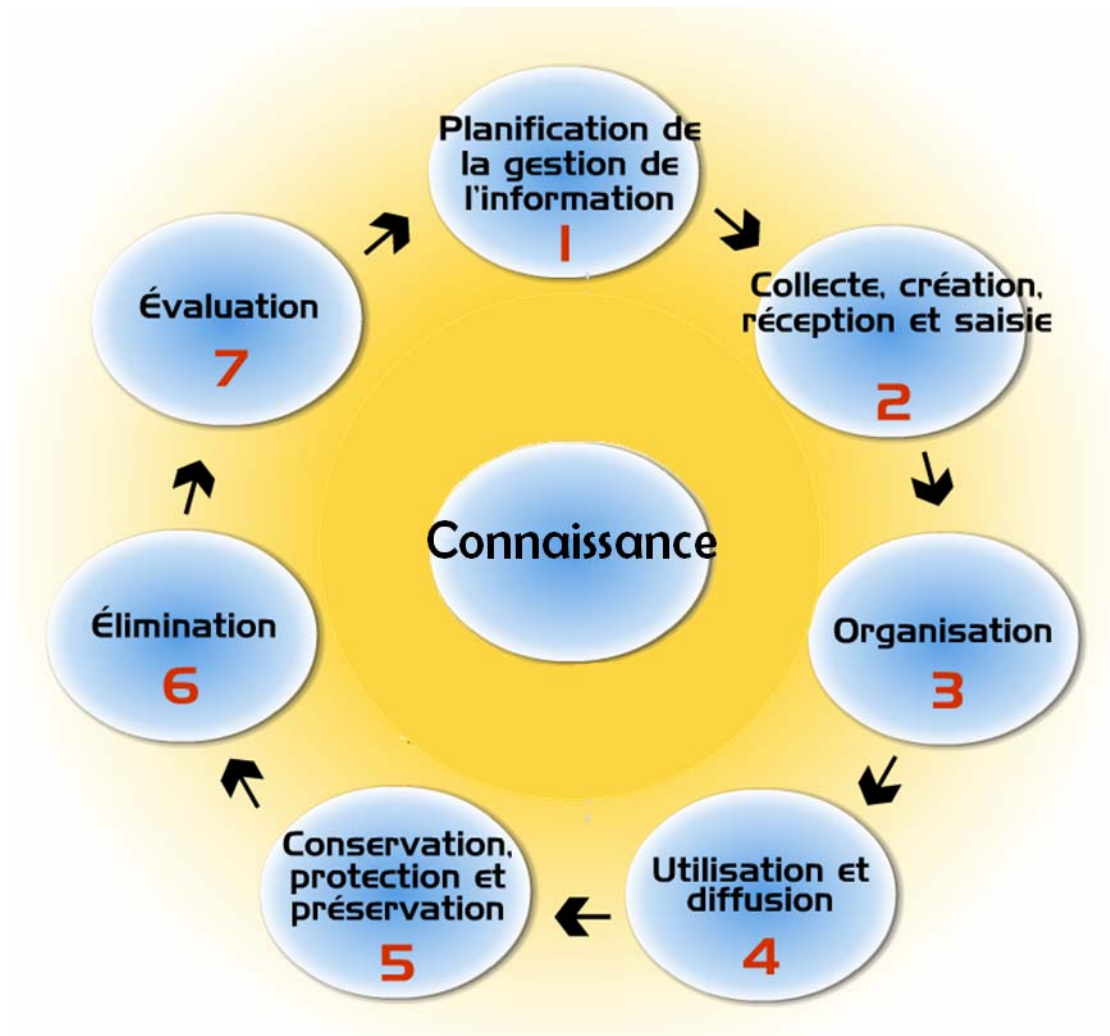
Utilisation et diffusion

Maintenance, protection et conservation

Élimination

Évaluation

Le diagramme qui suit présente le cycle de vie de la gestion de l'information; les sept phases forment le pourtour du cycle. La connaissance qu'une personne a de ses propres responsabilités est cruciale; elle occupe le centre du cycle de vie.



Pour plus d'informations, veuillez consulter le site de Bibliothèque et Archives Canada :
(Source : <http://www.collectionscanada.ca/>)



0.9. Définitions

Administrateur de courriel (administrateur de système ou administrateur de réseau)

Personne responsable de la maintenance du système de courriel, incluant toutes les boîtes aux lettres de ce système.

Adresse de courriel

Suite de caractères permettant aux systèmes informatiques de faire parvenir un courriel à son destinataire; cette suite contient habituellement un nom d'utilisateur, le symbole @ et un nom de domaine (par exemple : jsmith@dept-dept.gc.ca).

Authenticité

L'authenticité d'un document réfère à sa fiabilité et son identité au fil du temps. L'authenticité garantit que le document n'a pas été modifié ou manipulé après sa création, sa réception ou sa migration tout au long du processus continu de création, de maintenance et de conservation.

Boîte aux lettres

Zone d'un système informatique où sont stockés les courriels reçus et expédiés par un utilisateur individuel.

Boîte d'envoi

Zone d'un système de courriel où sont stockés les courriels envoyés par un utilisateur. Habituellement, la boîte d'envoi n'est qu'une zone tampon où le courriel est gardé avant d'être envoyé (ce qui, la plupart du temps, se fait presque instantanément). Après l'envoi, une copie du courriel est stockée dans un dossier « Messages envoyés » ou disparaît complètement de la boîte aux lettres de l'expéditeur, selon les règles administratives en vigueur, lesquelles peuvent souvent être personnalisées par l'utilisateur.

Calendrier de conservation

Outil ou document de gestion qui indique les délais de conservation pour tous les documents d'une organisation. Ces délais peuvent varier selon les types de documents.



Compte de courriel

Boîte aux lettres d'un utilisateur et droits d'utilisation de cette boîte.

Copie latente

Lorsqu'un courriel est supprimé, il n'est pas détruit. Il reste sur le disque dur, la bande de sauvegarde ou le serveur tant qu'il n'est pas écrasé par un autre fichier. En fait, lorsqu'un message est « supprimé », c'est uniquement le pointeur électronique vers le message qui est détruit. Selon la capacité du support de stockage électronique, un courriel peut continuer d'exister sous forme de copie latente pendant plusieurs années avant qu'il ne soit finalement écrasé. Et même à ce moment-là, il sera peut-être encore possible de le récupérer, en tout ou en partie, à l'aide d'une technologie appropriée.

Copie officielle

Ce terme sert à désigner la version d'un document censée être la version originale ou définitive, authentique et fiable à des fins légales.

Courriel

- Système informatique permettant à l'utilisateur de créer, d'expédier, de recevoir, de classer et de répondre à des messages électroniques.
- Message créé, expédié, reçu ou retransmis grâce à réseau électronique.

Courriel non considéré comme un document organisationnel

Aux fins des présentes lignes directrices, n'est pas considéré comme un document organisationnel, tout courriel contenant des informations qui ne sont pas reliées aux activités d'une institution gouvernementale, ou tout type d'information qui n'est pas un document officiel (p. ex., une publication externe, un formulaire vierge ou un manuel d'entretien). Les types de courriels suivants, et les pièces qui y sont jointes, ne sont pas considérés comme des documents organisationnels :

Correspondance personnelle

- Courriels échangés avec des amis ou des membres de la famille
- Courriels envoyés ou reçus concernant les activités personnelles d'un utilisateur
- Copies d'annonces reçues



- Courriels relatifs à des collectes de sang, des activités de bienfaisance, des événements sociaux ou sportifs auxquels les employés de l'institution sont invités

Documents publiés par d'autres organismes ou entreprises, accessibles au grand public et qui ne font pas partie d'un document cas ou d'une proposition d'achat

- Catalogues, prospectus ou brochures électroniques
- Journaux, magazines ou livres électroniques
- Matériel promotionnel non sollicité (pourriels)
- Fichiers copiés ou téléchargés à partir de sites Internet

Courrier électronique

Voir « Courriel »

Découverte

La découverte est l'une des étapes d'une action en justice, durant laquelle chacune des parties doit produire toutes les preuves pertinentes au litige en question et qui relèvent de son contrôle. Ceci inclut toute preuve qu'une partie peut utiliser pour défendre son point de vue, ainsi que toute information pouvant être utilisée contre la partie adverse, ou que la partie adverse peut utiliser pour défendre son propre point de vue. En principe, un courriel peut être « découvert » et exigé par la cour aussi longtemps qu'il continue d'exister (voir « Copie latente »).

Délai de conservation

Période de temps durant laquelle un document doit être conservé à des fins administratives, fiscales, juridiques ou historiques.

Document

1. « Éléments d'information, quel qu'en soit le support; la présente définition ne vise pas les publications ». (Loi sur la Bibliothèque et les Archives du Canada, 2004, Loi à jour en date du 13 juin 2008)
2. « Sont assimilés à une pièce l'ensemble ou tout fragment d'un livre, d'un document, d'un écrit, d'une fiche, d'une carte, d'un ruban ou d'une autre chose sur ou dans lesquels des renseignements sont écrits, enregistrés, conservés ou reproduits, et, sauf pour l'application des paragraphes (3) et (4), toute copie ou transcription admise en preuve en vertu du présent article en conformité avec le paragraphe (3) ou (4) ». (Loi sur la preuve au Canada, 1985, Loi à jour en date du 13 juin 2008)



3. « Éléments d'information, quel qu'en soit le support (Loi sur l'accès à l'information, 1985, Loi à jour en date du 13 juin 2008)

Aux fins de ces lignes directrices, un document contient de l'information relative à une transaction effectuée, une décision prise ou une action menée dans le cadre des activités d'une institution gouvernementale, notamment de l'information qui est déterminante (ou considérée comme telle) dans le processus.

Document officiel

Document créé ou reçu dans le cours normal des activités d'une organisation, par exemple, pour effectuer une transaction, fournir un service, prendre une décision ou mener une action conformément à ses responsabilités et à son niveau d'autorité, en vertu du mandat d'une institution gouvernementale.

Documents essentiels

Certains documents sont essentiels à la poursuite ou au rétablissement des activités vitales de l'institution. Ces sont notamment les documents qui :

- pourraient affecter les droits fondamentaux des personnes et des organisations, tels que les droits légaux, les droits de propriété, etc.;
- sont les plus utilisés et les plus demandés;
- exigeraient un investissement énorme en temps, en argent et en ressources humaines s'ils devaient être reconstitués avec leurs systèmes associés;
- sont similaires à ceux qui ont été inclus par d'autres institutions fédérales dans leur programme de gestion des documents essentiels;
- doivent être conservés en vertu d'une loi ou d'un règlement.

Indexation

Processus par lequel des mots-clés, des expressions et des termes sont utilisés pour faciliter l'identification d'un courriel ou de ses pièces jointes afin de pouvoir le repérer et le récupérer plus tard.

Information ou document éphémère

Les informations éphémères se trouvent dans les documents (éphémères) dont on a besoin seulement pendant une période de temps limitée, afin d'effectuer des activités courantes ou de préparer d'autres documents. Les documents éphémères ne comprennent pas les documents ayant une valeur historique, ni les documents nécessaires aux institutions fédérales ou aux ministres



pour contrôler, appuyer ou documenter la réalisation de programmes, pour effectuer des opérations, prendre des décisions, ou rendre compte des activités du gouvernement.

Voici quelques exemples d'informations éphémères que l'on retrouve dans les courriels :

- Nouvelles diffusées via divers médias par voie de courriel ou de communiqués internes, par exemple
- Communiqués
- Avis à l'ensemble du personnel, annonces d'événements spéciaux
- Demandes relatives à la tenue d'une réunion
- Offres de formation
- Invitations
- Messages personnels
- Photos en format JPEG, GIF, ou autre
- Messages à titre informatif (PVI – pour votre information)
- Annonces, journaux, livres, brochures, bulletins ou rapports publiés en format électronique
- Courriels imprimés sur papier ou saisis dans un système de classement électronique
- Demandes d'information de routine
- Avis (départ en vacances, campagnes de sollicitation, etc.)
- Anciennes versions de documents de travail

Intégrité

L'intégrité fait référence à la fiabilité et à la fidélité des documents, qu'il s'agisse d'originaux, de reproductions ou de représentations comparables de documents électroniques. L'intégrité fait aussi référence à la fiabilité et à la fidélité du système de gestion des documents dans lequel les documents électroniques sont enregistrés ou stockés pour produire des copies et des duplicatas fiables et fidèles de ces documents.

Lignes directrices pour la gestion des courriels

Les lignes directrices pour la gestion des courriels sont des règles, des pratiques et des exigences mesurables qui servent de modèle pour la gestion des courriels, de leurs métadonnées et pièces jointes.

Liste de diffusion

Liste d'adresses électroniques servant à envoyer des courriels à plusieurs personnes à la fois.



Loi et règlements sur l'AIPRP et demande d'accès en vertu de l'AIPRP

Le sigle AIPRP désigne l'accès à l'information et la protection des renseignements personnels; il est souvent employé pour identifier les demandes d'accès formulées en vertu de cette législation. L'accès à l'information est le principe général selon lequel les Canadiens peuvent demander à consulter des dossiers du gouvernement fédéral. Cet accès est parfois restreint, par exemple dans le cas où l'information demandée contient des renseignements personnels sur un individu (autre que celui qui fait la demande).

Mémoire institutionnelle - documents

Documents officiels découlant des fonctions et activités d'une institution gouvernementale, en vertu de son mandat, de son encadrement législatif, et des programmes et services qu'elle offre. Ces documents, qui constituent la mémoire institutionnelle, peuvent être créés ou utilisés à diverses fins.

- Offrir différents programmes et services
- Documenter des activités financières ou administratives
- Traiter diverses questions d'ordre juridique
- Prendre ou documenter des décisions ayant des impacts sur les politiques, les programmes ou les procédures
- Rendre compte au Parlement
- Saisir et documenter des événements qui pourraient avoir une certaine importance historique
- Documenter le pourquoi et le comment des décisions prises ou des actions menées

Les documents constituant la mémoire institutionnelle sont soumis à des calendriers de conservation approuvés par l'organisme et par Bibliothèque et Archives Canada, et doivent être gérés par des systèmes officiels de gestion des documents. Ces documents ne peuvent être détruits sans une autorisation de disposition de documents émise par Bibliothèque et Archives Canada.

Mémoire institutionnelle - information

La mémoire institutionnelle se retrouve dans les documents officiels et les souvenirs que certaines personnes peuvent avoir conservé des activités de leur organisation, mais elle se trouve aussi sur divers formats et supports électroniques qui gardent la trace des opérations courantes et des processus décisionnels. Ces informations constituent des ressources importantes pour l'organisation, car elles représentent l'expérience, le savoir et la mémoire des individus qui y ont travaillé. La mémoire institutionnelle fournit les bases nécessaires pour prendre de bonnes décisions, et témoigne des raisons justifiant ces décisions, incluant les circonstances, le contexte et d'autres renseignements disponibles lors de la prise de décision. Le courriel est devenu une très



importante source de mémoire institutionnelle, même si, à ce jour, son plein potentiel a rarement été exploité de manière efficiente et organisée.

Message courriel

Document créé, transmis, reçu ou transféré dans un système électronique de courrier.

Métadonnées

Informations décrivant un ensemble de données (p. ex. : objet, date et destinataire d'un courriel).

Mot de passe

Chaîne de caractères habituellement choisie par un utilisateur, reconnaissable par le système informatique et utilisée en association avec un nom d'utilisateur, pour identifier et authentifier cet utilisateur et lui autoriser l'accès au système.

Serveur de courriel

Ordinateur en réseau qui fournit des services de courriel à d'autres ordinateurs de ce réseau.

Système de courriel

Système informatique comprenant des ordinateurs et des logiciels, utilisé essentiellement à des fins de communication; les utilisateurs peuvent créer, transmettre, recevoir, classer et répondre à des messages de manière électronique.

Un système de courriel n'est pas un système de gestion des documents et ne convient pas pour classifier, classer et stocker des messages électroniques (voir : Système de gestion des documents).

Plusieurs systèmes de courriel offrent aussi une fonctionnalité de calendrier, grâce à laquelle les utilisateurs peuvent fixer la date d'une réunion, réserver une salle ou de l'équipement, envoyer, accepter ou refuser une invitation. De plus, les systèmes de courriel permettent souvent aux utilisateurs de créer des listes de tâches à effectuer et de leur attribuer un ordre de priorité; certains sont même couplés à un système de messagerie sans fil ou de messagerie vocale. Les systèmes de courriel évoluent très rapidement.



Système de gestion de l'information

Travaux publics et Services gouvernementaux Canada (TPSGC) définit son système de gestion des dossiers, des documents et de l'information (SGDDI) comme « ... une suite d'applications conçue pour doter les ministères et organismes du gouvernement fédéral d'un logiciel économique de gestion des dossiers et des documents ».

(Source : <http://www.tpsgc.gc.ca/rdims/text/index-f.html>)

Système de gestion des documents

Un système de gestion des documents est un dépôt à long terme et des processus associés permettant d'entreposer, de conserver, de consulter et, finalement, d'éliminer des documents organisationnels d'une institution. Un tel système s'appuie sur des méthodes et des technologies pour l'entreposage des documents, tant sur support papier qu'en format électronique.

Threading

Mécanisme par lequel un système de gestion de l'information peut suivre à la trace les relations existant entre des courriels, leurs métadonnées et pièces jointes, à l'intérieur d'une suite de courriels.



1. Les institutions doivent se doter d'un plan pour gérer les courriels

Depuis une dizaine d'années, la gestion des courriels constitue l'un des plus importants défis à relever en gestion de l'information. Les organisations devront concevoir des plans d'ensemble détaillés, afin d'arriver à maîtriser la croissance phénoménale de ce moyen de communication électronique, avec sa gamme de plus en plus large d'utilisations, de caractéristiques et de fonctionnalités.

Le plan doit incorporer plusieurs composantes de la gestion des courriels, notamment :

- l'élaboration de politiques et procédures relatives à la gestion des courriels, en lien avec les activités de l'institution;
- une gestion intégrée des avantages et inconvénients du courriel, qui accordera une égale importance aux messages électroniques, à leurs métadonnées et pièces jointes, et permettra l'utilisation d'infrastructures communes et l'interopérabilité des systèmes de courriel et de gestion de l'information;
- la prise en compte, dès le départ, des exigences propres à la gestion des courriels lors de l'élaboration de nouveaux programmes, politiques, services et systèmes fondés sur la technologie;
- la mise en place de structures de gouvernance et de responsabilisation pour la gestion de l'information en général, et des courriels en particulier;
- des programmes de sensibilisation et de formation sous diverses formes.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Un plan détaillé de gestion des courriels sera appuyé et adéquatement financé par la haute direction.
- Le plan de gestion des courriels indiquera de quelle manière les Lignes directrices pour la gestion des courriels au gouvernement du Canada seront respectées.
- Chacune des recommandations relatives à la gestion des courriels sera considérée attentivement.
 - Si recommandation est adoptée, il en sera fait mention.
 - Si une recommandation doit être interprétée à la lumière du mandat de l'institution ou de son champ d'activités, cette interprétation sera fournie.



- Si une recommandation doit être adaptée au mandat de l’institution ou à son champ d’activités, la nature de cette adaptation sera indiquée.
- Si une recommandation ne s’applique pas, on en donnera la raison ou on proposera une autre recommandation.

1.1. Gérer les programmes et les systèmes de courriel de manière intégrée

Tous les programmes de courriel utilisés par les institutions, et les systèmes qui leur sont associés, devraient être financés adéquatement par la direction; ils devraient aussi être conçus et configurés de façon à leur permettre de saisir, stocker et gérer efficacement les courriels reçus et expédiés, avec leurs métadonnées et leurs pièces jointes.

Une sélection de courriels contenant des informations et des documents gouvernementaux devrait être extraite du reste des documents moins pertinents et conservée pendant une durée de temps appropriée, conformément au cycle de vie de la gestion de l’information recommandé dans la Politique sur la gestion de l’information.

Note : Dans le tableau ci-dessous, la cellule claire indique à qui appartient la responsabilité de mettre en oeuvre ou d’appliquer la recommandation.

Partie ou parties responsables de la mise en oeuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Un programme de gestion des courriels est bien plus qu’un ensemble de logiciels et d’équipements informatiques. Il suppose l’utilisation d’une infrastructure technologique, les efforts conjugués de nombreuses personnes, l’accès à des documents de référence et de formation, et le développement de savoirs et de compétences. Tous ces éléments doivent s’articuler efficacement, afin de bien identifier et saisir l’information et les documents gouvernementaux, et veiller à ce qu’ils soient préservés.

Une des prémisses à la base de tout système intégré de gestion des courriels est que le nombre de copies de courriels soit réduit au minimum. Cela simplifie considérablement les opérations de classement, de stockage, de récupération et de disposition. Mais il y a d’autres avantages. Par exemple, en vertu de la Loi sur la protection des renseignements personnels, toutes les copies de certains types de documents et d’informations doivent être détruites à l’expiration de leur délai de conservation. Il est évidemment bien plus facile de respecter cette obligation si les copies sont en nombre restreint, et si leur lieu de conservation est connu. De même, si un document est conservé



en un seul endroit, il est beaucoup plus facile de le repérer et de veiller à ce qu'il ne soit pas détruit, s'il doit être produit en preuve lors d'un audit ou d'une action en justice.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante concernant la gestion des courriels :

Choisir une des deux options suivantes :

Option 1. (Nom de l'institution) conserve une copie (une seule, outre la copie de sécurité), avec les métadonnées et les pièces jointes, cette copie étant considérée comme la copie officielle, dans un système partagé avec d'autres organismes du gouvernement fédéral.

Option 2. (Nom de l'institution) conserve une copie (une seule, outre la copie de sécurité), avec les métadonnées et les pièces jointes, cette copie étant considérée comme la copie officielle, dans un système qu'il gère lui-même.

Lorsqu'un courriel, provenant de l'organisme lui-même, contribue à une décision ou à une action, la copie officielle est celle qui est retirée du compte de courriel de l'expéditeur et stockée dans un dépôt autorisé, géré par l'organisme.

Lorsqu'un courriel reçu de l'extérieur contribue à une décision ou à une action de son destinataire à l'intérieur de l'organisme, la copie officielle est celle qui est retirée ou copiée du compte de courriel de la personne principalement responsable de prendre ou d'obtenir cette décision, ou d'entreprendre cette action.

Aux fins de cette politique, le programme de gestion des courriels de (nom de l'institution) comprend plusieurs composantes interreliées.

- Infrastructure technique
 - Ordinateurs, logiciels, réseaux, mécanismes de sécurité en TI
 - Stockage électronique en ligne (habituellement géré par le système de courriel lui-même, pour le stockage de courte durée)
 - Systèmes de secours
 - Système à mémoire non intégrée et système hors ligne pour la conservation de longue durée
 - Mécanismes de migration des données – afin que les courriels et leurs pièces jointes demeurent accessibles aussi longtemps que nécessaire, sans égard à l'évolution ou à l'obsolescence technologiques, et comme mesure de protection contre la détérioration physique des supports de conservation
 - Zones d'attente ou technologies de compilation utilisées pour assembler, préparer et livrer des courriels à Bibliothèque et Archives Canada à des fins de conservation permanente
- Infrastructure en ressources humaines
 - Une ou des personnes, possédant idéalement une formation spécialisée, responsables de la gestion de l'information et des technologies de l'information
 - Des dirigeants pour établir la politique et des gestionnaires pour évaluer les besoins en matière de formation, offrir cette formation et veiller au respect de la politique.
 - Des utilisateurs qui sont en mesure de décider quels messages conserver, pour combien de temps et à quel endroit. Dans certains cas, le choix est restreint et assisté par ordinateur.
- Infrastructure cognitive
 - Politiques, procédures, lignes directrices, formation
- Infrastructure de gestion
 - Ordres de retenue



1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels

Des programmes de sensibilisation et de formation à la gestion des courriels devraient être mis sur pied afin d'aider les employés à développer les connaissances et habiletés qui leur permettront d'utiliser le courriel de manière efficace et appropriée.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Plusieurs lois et politiques exigent la création de documents. Une bonne stratégie pour éviter aux institutions gouvernementales le lourd fardeau de la découverte électronique, consiste à former les employés à « rédiger tous leurs documents comme si ces derniers devaient un jour faire l'objet d'un examen par un juge ou un jury ».

De plus, on attend des utilisateurs qu'ils maîtrisent plusieurs autres fonctionnalités du système de courriel, mais ces dernières font rarement l'objet de formations structurées. Un des meilleurs moyens de garantir une gestion efficace des courriels est d'offrir au personnel une formation rigoureuse. Un bon programme de formation doit proposer différents modes d'apprentissage. Certains préfèrent l'auto-apprentissage, d'autres les cours formels en classe. Certains ont besoin de voir et d'expérimenter plutôt que de lire et d'écouter, mais tous doivent renforcer leurs apprentissages par de fréquentes répétitions.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : une formation sur la gestion et l'utilisation du courriel sera élaborée et offerte, afin d'apprendre aux participants à réaliser les activités suivantes.

- Utiliser le système de courriel de manière appropriée, efficace et efficiente
- Utiliser le système de courriel de manière courtoise et attentionnée (Nétiquette)
- Créer, utiliser et protéger des mots de passe
- Adopter des pratiques sécuritaires en matière de courriel à toutes les étapes du cycle de vie de l'information
- Savoir reconnaître les courriels qui constituent de l'information ou des documents à conserver



- Savoir reconnaître les courriels qui ne constituent pas des documents à conserver, et les effacer dès qu'ils n'ont plus aucune utilité
- Appliquer les dispositions légales ou réglementaires concernant la préservation des documents gouvernementaux
- Conserver les documents et l'information (courriels, métadonnées et pièces jointes) pendant la période de temps appropriée
- Appliquer les dispositions légales ou réglementaires concernant la protection des renseignements personnels et la confidentialité
- Disposer des documents et de l'information à l'expiration de leur délai de conservation
- Appliquer les dispositions de la Loi sur le droit d'auteur
- Classifier les courriels et les classer au bon endroit
- Sélectionner et transmettre à Bibliothèque et Archives Canada les fichiers de courriels appropriés, au moment opportun
- Savoir reconnaître qui a la responsabilité de conserver les courriels (expéditeur, destinataire, ou les deux)
- Gérer adéquatement leurs propres courriels, et, s'il y a lieu, des boîtes aux lettres communes ou publiques
- Reconnaître les différents rôles des utilisateurs, des spécialistes et des gestionnaires en matière de gestion de courriels
 - Dirigeants, administrateurs et gestionnaires des organismes
 - Utilisateurs du système de courriel
 - Spécialistes en gestion de l'information
 - Spécialistes en technologie de l'information, incluant les administrateurs de réseaux et de systèmes

1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels

Divers supports devront être utilisés afin que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et les procédures associées soient bien comprises et mises en œuvre dans l'organisation.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Pour être vraiment efficace, un bon programme de formation doit proposer plusieurs modes d'apprentissage à l'aide de différents supports, car les styles d'apprentissage varient selon les individus. Certains préfèrent la lecture et l'auto-apprentissage à l'ordinateur, d'autres les cours en classe. Certaines personnes auront besoin de rappels à leur écran.

De plus, il est important de répéter et de renforcer les points saillants de la formation. Changer de support permettra d'attirer plus efficacement l'attention des participants.



La formation devra également être adaptée au public cible. Tout le monde dans l'institution aura besoin d'une certaine forme d'apprentissage à l'utilisation des courriels. Cependant, il faudra concevoir des formations sur mesure pour les dirigeants, les gestionnaires, les spécialistes en gestion de l'information et les administrateurs de réseaux et de systèmes, afin de tenir compte des responsabilités très différentes de chacun de ces groupes.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : la formation en gestion des courriels doit être offerte dans une variété de supports, afin d'accommoder différents styles d'apprentissage et renforcer les messages clés en gestion des courriels. Cette politique vise à garantir que les Lignes directrices, les politiques et procédures, ainsi que les rôles et responsabilités en matière de gestion des courriels soient bien compris et appliqués de manière uniforme par le personnel de l'institution.

1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, ont été bien distribuées, lues et comprises

Chaque institution devra distribuer les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, afin que les dispositions contenues dans ces documents soient bien connues et comprises de tous ses employés, contractuels et autres utilisateurs relevant de son autorité.

L'institution devra également informer ses employés, contractuels et autres utilisateurs qu'elle attend d'eux qu'ils se conforment aux Lignes directrices pour la gestion des courriels et à toutes les recommandations adoptées par l'institution, et qu'un usage abusif du système de courriel peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement ou à la résiliation d'un contrat.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Il existe différents moyens de vérifier que les Lignes directrices pour la gestion des courriels ont bien été lues et comprises. En voici quelques-uns :



- administration de tests;
- simple signature sur un document reconnaissant que l'information a été lue et comprise;
- surveillance de la conformité.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution veillera à ce que les employés, les contractuels et les autres utilisateurs à son emploi soient bien informés et comprennent les dispositions contenues dans les Lignes directrices pour la gestion des courriels, ainsi que toutes les recommandations applicables.

Les employés, contractuels et autres utilisateurs sont, par les présentes, informés que l'institution s'attend à ce qu'ils se conforment aux Lignes directrices pour la gestion des courriels, et que tout usage abusif du système de courriel peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement ou à la résiliation d'un contrat.

L'institution devrait utiliser l'une ou l'autre des méthodes suivantes afin de garantir que les Lignes directrices pour la gestion des courriels et les recommandations applicables ont été lues et comprises.

Choisissez la ou les méthodes applicables parmi les suivantes :

- L'institution obtiendra de chaque employé, contractuel ou autre utilisateur, une simple signature sur un document reconnaissant que l'information a été lue et comprise.
- Les employés, contractuels et autres utilisateurs devront passer un test pour confirmer qu'ils ont bien compris les principes clés de la gestion du courriel, ainsi que leurs propres rôles et responsabilités en la matière.
- Les comptes de courriels des employés, contractuels et autres utilisateurs seront surveillés (selon une méthode aléatoire ou autre) pour garantir la conformité.

1.5. Conserver des dossiers sur les activités de formation et sur la participation

Les institutions devraient conserver des dossiers sur les activités de formation en gestion des courriels, ainsi que sur l'assistance à tout atelier, cours en classe ou présentation sur le sujet. Ces dossiers devraient être conservés pendant une longue période de temps afin de pouvoir être consultés, au besoin, dans le cadre d'un audit ou d'une action en justice.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de	Spécialistes en gestion de	Gestionnaires des opérations	Dirigeants
--------------	----------------------------------	----------------------------	------------------------------	------------



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

	systemes	l'information		
--	----------	---------------	--	--

Justification

Les dossiers documentant les activités de formation en gestion des courriels offertes par l'institution, ainsi que les dossiers concernant l'assistance à des programmes de formation en la matière, peuvent être utilisés en cour pour justifier la qualité et l'envergure des programmes de formation de l'institution. Comme tels, ils peuvent ajouter du poids aux éléments de la preuve par courriel produite par l'institution.

De tels dossiers peuvent aussi être utilisés lors d'actions en justice pour réfuter des allégations voulant qu'un ou plusieurs utilisateurs au sein de l'institution n'aient pas reçu de formation appropriée en gestion des courriels. Si ces utilisateurs sont inscrits à une séance de formation, il sera difficile de démontrer qu'aucune formation ne leur a été offerte.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution conservera des dossiers sur les activités de formation en gestion des courriels offertes aux employés, contractuels et autres utilisateurs, et sur l'assistance aux séances de formation, en demandant aux participants de signer à côté de leur nom sur une feuille de présence. Ces dossiers devront être conservés pendant une longue période de temps.



2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles

Conformément à la Politique sur la gestion de l'information, les institutions sont tenues de recueillir, créer, recevoir et conserver tous les courriels relatifs à leurs activités organisationnelles, notamment les courriels contenant des informations constitutives de la mémoire institutionnelle et des données servant à prendre une décision ou à entreprendre une action visant à :

- soutenir la prestation de services, l'élaboration de politiques judicieuses et la prise de décisions éclairée, et répondre aux exigences organisationnelles, juridiques et de reddition de comptes;
- assurer la pertinence, la fiabilité et l'exhaustivité de l'information;
- optimiser le partage et la réutilisation de l'information conformément aux obligations découlant des lois et des politiques;
- documenter les décisions et les processus décisionnels pour rendre compte des activités du gouvernement, reconstituer l'évolution des politiques et des programmes, assurer la continuité du gouvernement et de son processus décisionnel, et permettre une vérification et un examen indépendants;
- réduire le fardeau des réponses aux demandes d'accès à l'information et aux demandes de preuves légales en évitant la collecte inutile de renseignements.

La gestion de tous ces documents soulève des questions fondamentales, notamment, combien d'exemplaires d'un document devrait-on conserver. Plus il y a d'exemplaires d'un même document, plus il y a d'endroits où ils peuvent se trouver, et plus il est difficile de les gérer. Afin de faciliter l'étape suivante du cycle de vie des documents (l'organisation), il est très important de conserver les métadonnées, c'est-à-dire les informations relatives aux courriels. Ces métadonnées peuvent comprendre le nom de l'expéditeur et le nom des destinataires, la date d'envoi du courriel, sa date de réception, l'objet du message et plusieurs autres informations pouvant servir à classer et à repérer le courriel ultérieurement.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Tous les utilisateurs du courriel vont créer, expédier, recevoir, réacheminer et stocker leurs courriels conformément aux présentes Lignes directrices pour la gestion des courriels, et à toutes les recommandations applicables.

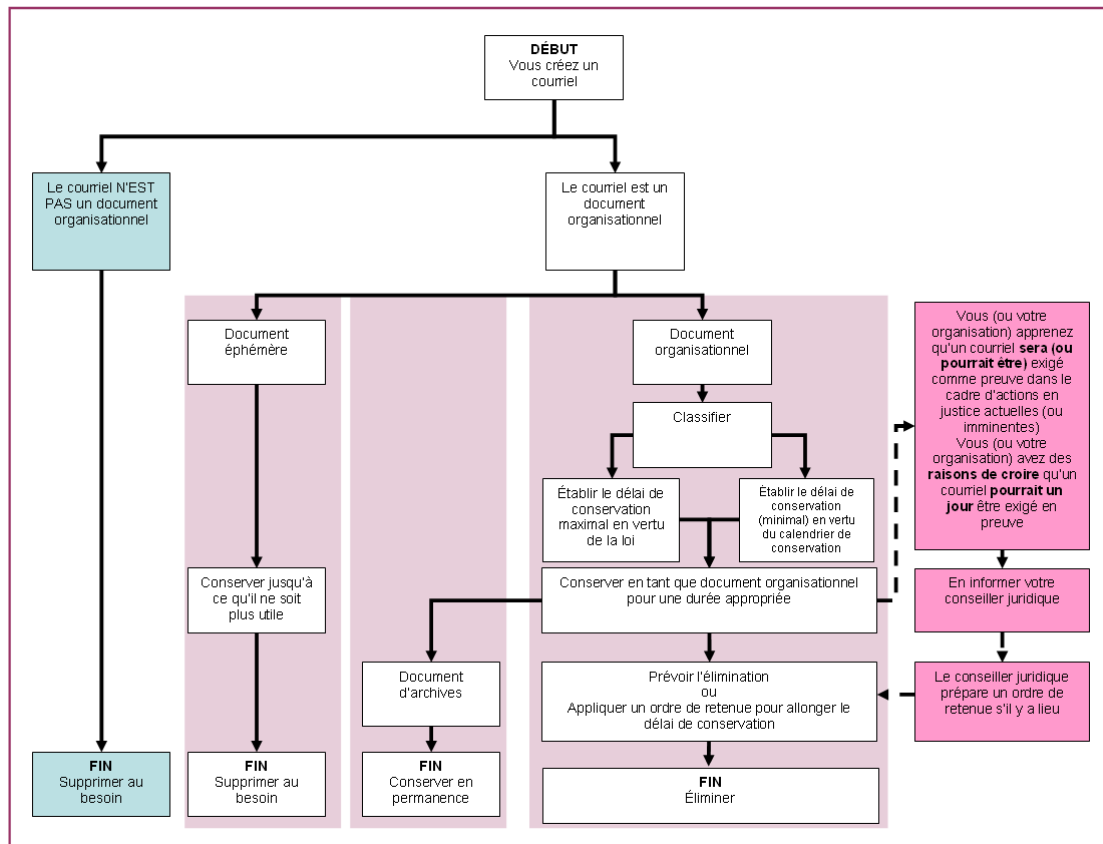


- Les employés sauront quels messages conserver ou éliminer, et se chargeront de gérer leurs propres boîtes aux lettres et leurs propres dossiers sur une base régulière.
- Un seul exemplaire d'un courriel sera conservé, dans un dépôt autorisé, où il aura le statut de « copie officielle ».
- Les pièces jointes seront stockées avec le message ou, sinon, seront liées au message de manière fiable.
- Les métadonnées associées aux courriels seront conservées.

2.1. Créer, expédier et stocker les courriels de manière structurée

Tout message contenant de l'information utilisée dans (ou considérée dans, ou concernant) une transaction effectuée, une décision prise ou une action entreprise dans le cadre des activités organisationnelles d'une institution gouvernementale doit être conservé.

Le diagramme suivant illustre le processus recommandé pour créer, expédier et stocker les courriels au gouvernement du Canada.

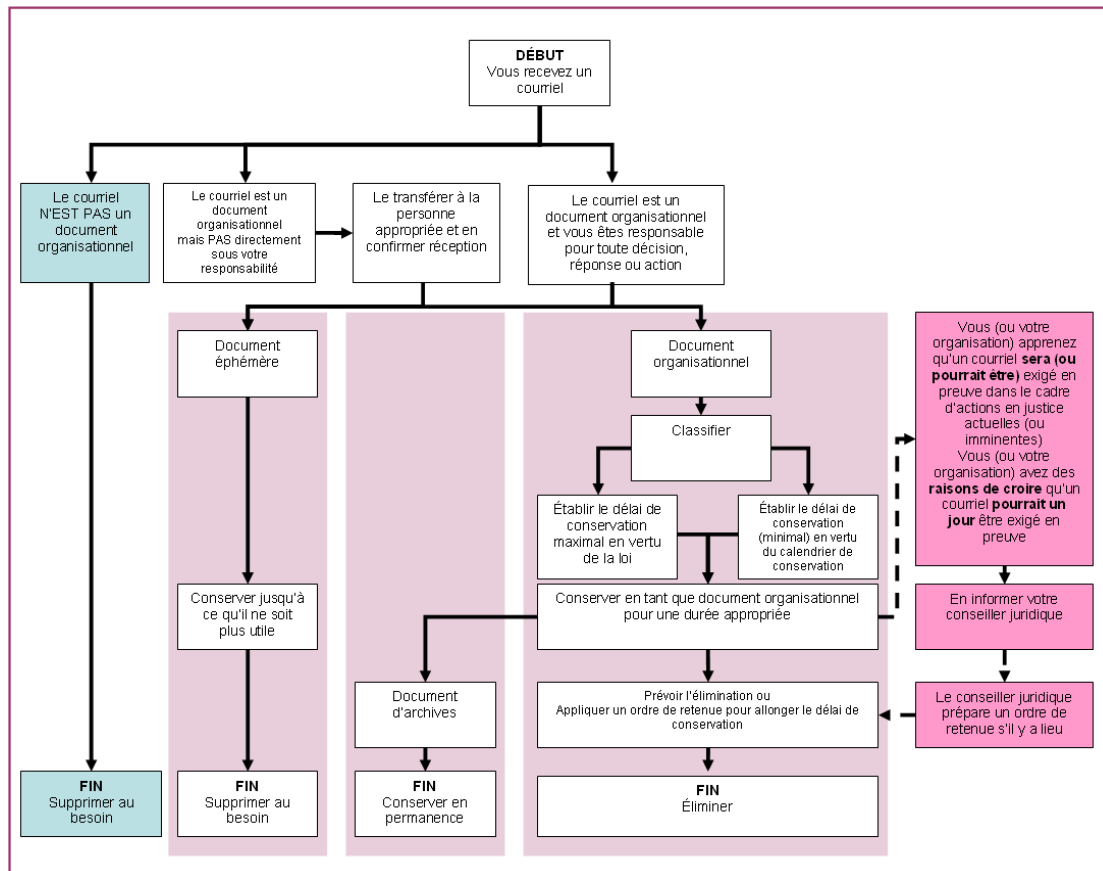


Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.2. Recevoir et stocker les courriels de manière structurée

Tout message reçu, contenant de l'information utilisée dans (ou considérée dans, ou concernant) une transaction effectuée, une décision prise ou une action entreprise dans le cadre des activités organisationnelles d'une institution gouvernementale doit être conservé.

Le diagramme suivant illustre le processus recommandé pour recevoir et stocker les courriels dans les institutions.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière

Pour gérer les boîtes aux lettres (boîtes de réception, messages envoyés, messages supprimés), les courriels devraient être régulièrement classifiés et placés dans un dossier approprié. Les courriels éphémères peuvent être placés dans la corbeille (messages supprimés).



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les boîtes aux lettres individuelles deviennent rapidement surchargées. Le tri des courriels est une tâche fastidieuse, mais nécessaire, et la remettre à plus tard ne la rend pas plus facile. Il est préférable de trier régulièrement ses courriels, de les classer et de les stocker dans les dossiers appropriés. Trier de plus petites quantités de messages prend moins de temps et semble moins déranger le « vrai travail ». En procédant ainsi, l'utilisateur sera en mesure de repérer l'information plus facilement et plus efficacement lorsqu'il en aura besoin.

À l'échelle d'une institution, le coût nécessaire pour retrouver un courriel isolé, ou un groupe de courriels, parmi des milliers ou même des millions de messages peut être extrêmement élevé. Si aucun système de classement approprié n'est utilisé, il faudra probablement mener des recherches à grands frais dans les bandes de sauvegarde, les disques durs de l'utilisateur, différents serveurs, et ainsi de suite. Bref, il n'y a pas vraiment d'alternative. Les courriels doivent être gérés, classifiés et stockés au bon endroit et de la bonne manière.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les courriels doivent être classifiés et classés systématiquement et régulièrement, à une fréquence appropriée à la nature des activités de (nom de l'institution), et conformément au système de classification adopté par (nom de l'institution). Les courriels doivent ensuite être stockés dans un dépôt désigné par l'institution.

Les messages personnels ou éphémères doivent être supprimés à volonté. Les courriels, les métadonnées et les pièces jointes qui contiennent de l'information ou des documents gouvernementaux doivent être placés dans un dépôt autorisé, et doivent être conservés durant une période de temps appropriée. Le gestionnaire de l'information doit offrir des orientations sur la façon de créer un dépôt, sur les délais de conservation à respecter pour certains documents, et sur la manière d'en disposer.

Les courriels, les métadonnées et les pièces jointes seront stockés dans un format compatible avec les activités organisationnelles de l'institution et classés conformément aux pratiques adoptées par l'institution ou par l'utilisateur.



2.4. Garder un seul exemplaire de chaque courriel

Dans la mesure du possible, les organisations ne devraient conserver, à titre de document officiel, qu'un seul exemplaire d'un courriel (outre la copie de sécurité), avec ses métadonnées et pièces jointes, dans un dépôt qu'elles gèrent ou contrôlent. Le logiciel de courriel lui-même doit être considéré comme un dispositif de communication et non de stockage. Les courriels devraient être transférés le plus rapidement possible dans un dépôt de documents indépendant. Puisque toute copie d'un courriel conservée peut être recherchée dans le cadre d'une action en justice, aucune autre copie de ce courriel ne devrait être conservée dans un autre dépôt ou par un individu dans l'organisation. La fonction « supprimer » élimine le pointeur électronique vers un courriel, mais ne détruit pas le message lui-même. Le message continue d'exister tant qu'il n'est pas écrasé par de nouvelles données.

Par exemple, un courriel ne devrait pas être conservé sur le disque dur d'un utilisateur. Une copie d'un courriel pourrait toutefois être stockée temporairement sur une clé USB ou sur le disque dur d'un ordinateur portable aux fins d'une présentation, mais elle devrait être effacée de manière sécuritaire après la présentation.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Il est beaucoup plus facile de gérer un seul exemplaire d'un courriel que plusieurs copies. Si un courriel doit être éliminé en raison de son contenu, ou produit à des fins juridiques, il est plus facile de répondre à des obligations découlant de lois ou de politiques s'il n'y a qu'un seul exemplaire du courriel à trouver et/ou à détruire. Si un document doit être produit dans le cadre d'une action en justice, d'un audit ou d'une demande en vertu de l'AIPRP, il sera plus facile de le repérer s'il n'y a qu'un seul endroit où chercher.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution ne conserve, à titre de document officiel, qu'un seul exemplaire d'un courriel (outre la copie de sécurité), avec ses métadonnées et pièces jointes. Cet exemplaire unique doit être transféré le plus rapidement possible vers un dépôt approprié, géré ou contrôlé



par (nom de l'institution). Le logiciel de courriel lui-même doit être considéré comme un dispositif de communication et non de stockage. Aucune autre copie du courriel ne devrait être conservée dans un autre dépôt ou par un individu dans l'organisation.

2.5. Gérer et conserver les pièces jointes aux courriels

Aux fins des présentes Lignes directrices pour la gestion des courriels, un système de gestion des courriels devrait conserver ensemble, dans le même dépôt, un message et sa ou ses pièces jointes, et être en mesure de prouver de manière fiable la relation existant entre ces documents.

Un système de gestion des courriels pourrait, aussi, conserver un message et ses pièces jointes dans des dépôts séparés, pourvu qu'il puisse fournir une preuve fiable qu'ils sont interreliés.

Les pièces jointes doivent être dans un format électronique pouvant être rattaché à un courriel : enregistrement audio, vidéo, message vocal, carte, graphique, photo numérique, feuille de calcul, base de données, présentation, texte, etc.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les courriels et leurs pièces jointes sont reliés, ils se complètent et s'expliquent mutuellement. Si un courriel et sa pièce jointe contribuent à une décision ou à une action causant un préjudice, le jugement de la cour concernant la faute ou la responsabilité peut dépendre de la nature de cette relation. La cour pourrait en arriver à un jugement différent selon que le message et la pièce jointe sont considérés isolément, ou ensemble.

Par conséquent, lorsqu'un courriel ou ses pièces jointes sont considérés comme une information ou un document gouvernemental, il est important de les conserver ensemble, durant une période de temps appropriée, avec les métadonnées qui établissent la nature de leur relation.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

Choisissez une de ces deux options :

Option 1. (Nom de l'institution) adopte la politique suivante : le système de gestion des courriels devrait conserver ensemble dans un même dépôt, un courriel et sa ou ses pièces jointes, et fournir une preuve fiable de la relation qui les unit.

Option 2. (Nom de l'institution) adopte la politique suivante : le système de gestion des courriels peut conserver un courriel et sa ou ses pièces jointes dans des dépôts séparés, mais en fournissant une preuve fiable de la relation qui les unit.

2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada

Les employés et les contractuels qui utilisent le système de courriel d'une institution fédérale devraient être informés que les courriels qu'ils créent, expédient ou reçoivent grâce à ce système ne leur appartiennent pas, que ces courriels peuvent être surveillés par l'institution et qu'ils ne devraient pas être considérés comme des messages personnels, de nature privée.

Tous les courriels, métadonnées et pièces jointes créés, reçus ou conservés par un système de courriel, une bande de sauvegarde, un serveur ou un autre moyen de stockage sous le contrôle d'une institution fédérale (incluant les ordinateurs portatifs, les clés USB, les CD et autres moyens de stockage portatifs) sont considérés comme la propriété de l'institution et devraient être traités comme tels.

Tout courriel créé, expédié ou reçu par un employé utilisant le système de courriel d'une institution fédérale est considéré comme étant sous le contrôle et la propriété de l'institution, peu importe l'endroit où il est conservé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	---	------------------------------	------------



Justification

Tous les documents ou les informations que contiennent les courriels, les métadonnées et les pièces jointes appartiennent à l'institution.

Certains organismes autorisent un usage personnel limité du courriel, pourvu que cette pratique ne nuise pas aux activités du gouvernement, ou ne représente pas un conflit d'intérêts. Cependant, cela ne signifie pas que les messages personnels sur un système de courriel gouvernemental sont de nature privée ou qu'ils « appartiennent » à l'employé qui les a envoyés ou reçus.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : tous les courriels, métadonnées et pièces jointes créés, reçus ou conservés par un système de courriel, sur une bande de sauvegarde, un serveur ou un autre moyen de stockage sous le contrôle d'une institution fédérale (incluant les ordinateurs portatifs, les clés USB, les CD et autres moyens de stockage que les employés peuvent apporter à la maison) sont considérés comme la propriété de (nom de l'institution) et doivent être traités en conséquence.

Les employés, contractuels et autres utilisateurs du système de courriel sont, par les présentes, informés qu'un courriel envoyé ou reçu par un employé à l'aide du système de courriel de (nom de l'institution) est toujours considéré comme appartenant à cette institution, même s'il s'agit d'une copie que l'employé garde à son domicile ou dans un autre endroit, après avoir supprimé le courriel à son bureau.

Les employés, contractuels ou autres utilisateurs du système de courriel sont, par les présentes, informés que tout courriel qu'ils créent, expédient ou reçoivent à l'aide du système ne leur appartient pas, qu'il peut être surveillé par l'institution et ne doit pas être considéré comme un message personnel, de nature privée.

2.7. Utiliser avec modération les listes de diffusion institutionnelles

Les listes de diffusion destinées à l'ensemble de l'institution, ses directions, bureaux, divisions, etc. ne devraient être utilisées que par des personnes autorisées, à des fins officielles approuvées par la haute direction.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de	Spécialistes en gestion de	Gestionnaires des opérations	Dirigeants



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

	systèmes	l'information		
--	----------	---------------	--	--

Justification

La création de listes ou de « groupes » de diffusion est une pratique courante. Ainsi, quelqu'un pourrait créer une liste pour l'ensemble d'une organisation, ou pour une direction, une division ou un bureau régional. De telles listes ne devraient être utilisées qu'à des fins officielles, par des personnes autorisées, et pour diffuser des messages approuvés par la haute direction.

Les longues listes de diffusion imposent un lourd fardeau au système de courriel et devraient servir uniquement à communiquer des informations importantes, intéressant un large public.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les listes de diffusion destinées à l'ensemble de l'institution, à une direction ou à une division, ne seront utilisées que par des individus ou des groupes autorisés, à des fins approuvées par la haute direction.

Le groupe chargé des communications internes à la direction des communications, le bureau administratif de chaque direction et le bureau du directeur de chaque division sont, par les présentes, autorisés à utiliser les listes de diffusion destinées à l'ensemble de l'institution, à une direction, à une division ou à un édifice en particulier aux fins suivantes :

- Alertes concernant la sécurité (type et envergure à déterminer)
- Événements (collectes de sang, campagnes d'œuvres de bienfaisance approuvées, activités sociales) impliquant le ministère, la direction ou la division
- Information relative aux ressources humaines (nomination de nouveaux dirigeants, relations de travail) impliquant le ministère, la direction ou la division
- Annonces d'ordre général (rénovations, réparations ou entretien du bureau) impliquant le ministère, la direction ou la division
- Autres (à déterminer)

Des personnes à tous les niveaux hiérarchiques de l'institution sont autorisées à créer et à tenir à jour des listes de diffusion pour les aider à réaliser les activités de l'institution. Les listes de diffusion peuvent être créées pour des groupes de travail, des équipes de projets, et des groupes d'intérêt (sécurité des technologies de l'information, gestion du risque, analyse opérationnelle, etc.).



2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource

Conformément à la politique de normalisation des sites internet du gouvernement du Canada (<http://www.tbs-sct.gc.ca/clf2-nsi2/index-fra.asp>), tous les courriels envoyés par les employés du gouvernement doivent indiquer le nom de l'expéditeur, le nom de son institution, ses numéros de téléphone et de télécopieur avec l'indicatif régional et le numéro du poste, ainsi que son adresse postale et son adresse de courriel. Tous les courriels envoyés par les employés du gouvernement doivent afficher de manière uniforme le mot-symbole « Canada » et la signature institutionnelle.

Certaines exemptions ou exceptions sont autorisées lorsque l'expéditeur a des motifs valables de vouloir préserver la confidentialité de ses messages, ou pour des raisons de sécurité personnelle, matérielle ou nationale.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Un courriel devrait toujours se terminer par les coordonnées de l'expéditeur; c'est une marque de professionnalisme et de courtoisie.

Cela évitera, par exemple, au destinataire d'un courriel qui préfère y répondre par téléphone, d'entreprendre de fastidieuses recherches pour trouver le numéro de son correspondant.

De plus, si le contenu du courriel réfère à un service ou à un programme offert par l'institution, le destinataire voudra peut-être obtenir plus d'informations à partir du site web de l'institution, avant de répondre à ce courriel par des commentaires ou des questions.

Certains types de renseignements ne devraient pas être envoyés par courriel, ou alors, sous forme chiffrée. Là où la technologie ne permet pas de chiffrer l'information, l'envoi par télécopieur constitue une alternative sécuritaire.. Là encore, l'indication du numéro de télécopieur dans le courriel facilitera la tâche au destinataire.

Comme principe général, si l'expéditeur du message occupe un poste bilingue, le titre et l'adresse de ce dernier devraient être fournis dans les deux langues officielles du Canada, en accordant la préséance à la première langue officielle de cette personne. Dans le cas d'un poste qui n'est pas



officiellement bilingue, l'adresse peut être indiquée dans une seule langue, la langue officielle associée à ce poste, indépendamment de la première langue officielle de son titulaire.

Certaines exceptions à ce principe pourraient s'avérer nécessaires. Pour des motifs personnels ou professionnels tout à fait légitimes, il peut être préférable de ne pas révéler le nom de l'expéditeur (au complet ou en partie) dans un bloc-signature.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les courriels envoyés par les utilisateurs, à l'intérieur comme à l'extérieur de l'organisme, devraient se terminer par un bloc-signature. Notez bien qu'il ne s'agit pas d'une signature « numérique » et qu'il n'offre aucun des mécanismes de sécurité normalement associés à la signature numérique.

Le bloc-signature doit comprendre le nom de l'expéditeur, son titre, le nom de son institution, ses numéros de téléphone et de télécopieur avec l'indicatif régional et le numéro du poste, ainsi que son adresse postale et son adresse de courriel. Lorsqu'il s'agit d'une adresse de courriel d'un programme ou d'un service plutôt que d'un individu, les coordonnées doivent comprendre le nom de l'institution, l'adresse postale et l'adresse de courriel, et les numéros de téléphone et de télécopieur. Tous les courriels envoyés par les employés du gouvernement doivent afficher de manière uniforme le mot-symbole « Canada » et la signature institutionnelle. Aucune autre image ou décoration n'est permise.

Comme principe général, le titre et l'adresse de l'expéditeur devraient être fournis dans les deux langues officielles, si la personne occupe est un poste bilingue, en accordant la préséance à la première langue officielle de cette personne. Dans le cas d'un poste qui n'est pas officiellement bilingue, l'adresse peut être indiquée dans une seule langue, laquelle sera la langue officielle associée à ce poste, indépendamment de la première langue officielle de son titulaire.

Tous les blocs-signature devraient être écrits avec la même police de caractères. Un modèle est disponible sur le site web de (nom de l'institution) à (adresse du site). Les utilisateurs pourront copier-coller le modèle, en suivant les instructions fournies sur le site, et substituer leurs nom, titre, adresse de bureau et numéros de téléphone et de télécopieur à ceux indiqués dans le modèle.

Certaines exemptions ou exceptions sont autorisées lorsque l'expéditeur a des motifs valables de vouloir préserver la confidentialité de ses messages, ou pour des raisons de sécurité personnelle, matérielle ou nationale. Dans ces cas, l'utilisateur devrait communiquer avec (nom du responsable de la sécurité) afin de s'assurer que toutes les mesures de sécurité appropriées ont été prises.



2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu

Les institutions doivent se demander s'il est approprié à leur situation d'insérer un avis de confidentialité ou de non-responsabilité sous le bloc-signature. En réfléchissant à cette question, l'organisme devrait procéder à une analyse de risque afin d'établir s'il est possible de limiter sa responsabilité. Voici un exemple d'un tel avis.

Avis de non-responsabilité

Ce courriel, incluant toute pièce jointe, s'adresse exclusivement à son destinataire et peut contenir des informations confidentielles ou privilégiées. (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du courriel et détruire tous les exemplaires de ce courriel. Merci.

La décision d'inclure ou non un tel avis de non-responsabilité (et la formulation exacte de cet avis) relève des dirigeants de l'institution, en consultation avec leurs conseillers juridiques.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

L'erreur est humaine. Il peut arriver, par exemple, qu'une personne sélectionne par inadvertance la mauvaise adresse de courriel dans une liste de diffusion et envoie un message au mauvais destinataire. Pour réduire les risques de responsabilité liés à un tel cas, certaines institutions pourraient décider d'ajouter un avis de confidentialité et de non-responsabilité invitant la personne qui reçoit le courriel à le détruire, si elle n'est pas le destinataire prévu. Une telle mesure de sécurité ne suffira pas à limiter la responsabilité dans toutes les circonstances. Les dirigeants de l'institution devraient consulter leurs conseillers juridiques pour évaluer les risques et choisir la meilleure ligne de conduite et, s'il y a lieu, rédiger un avis de non-responsabilité.

L'avis de non-responsabilité peut être appliqué automatiquement à l'ensemble de l'institution, ou se limiter à certains groupes d'utilisateurs. Un avis de non-responsabilité peut aussi être inséré manuellement par l'utilisateur, dans certaines circonstances, à condition que celui-ci connaisse bien les règles et les applique uniformément.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : un avis de confidentialité ou de non-responsabilité, est inséré sous le bloc-signature des courriels. L'avis de non-responsabilité vise à réduire les risques de responsabilité résultant de courriels envoyés à une personne ou une organisation autre que le destinataire prévu. L'avis de non-responsabilité doit (s'afficher automatiquement / être inséré manuellement par l'utilisateur). L'utilisation de l'avis de non-responsabilité doit (s'appliquer à l'ensemble de l'organisation / être limitée à certains groupes – en fournir la liste).

L'avis doit être affiché dans le format suivant (décrire ou fournir le format), et se lire comme suit : (fournir le texte exact de l'avis).

Avis de non-responsabilité

Ce courriel, incluant toute pièce jointe, s'adresse exclusivement à son destinataire et peut contenir des informations confidentielles ou privilégiées. (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du courriel et détruire tous les exemplaires de ce courriel. Merci.

2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu

Les institutions doivent examiner s'il est approprié à leur situation de demander aux utilisateurs d'insérer un avis d'opinion personnelle, dans certaines circonstances. Voici un exemple d'un tel avis.

Avis d'opinion personnelle

Ce courriel, incluant toutes les pièces jointes, reflète l'opinion personnelle de l'expéditeur et ne représente pas l'opinion ou la position officielle de (nom de l'institution). (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du courriel et détruire tous les exemplaires de ce courriel. Merci.



La décision d'inclure ou non un tel avis d'opinion personnelle (et la formulation exacte de cet avis) relève des dirigeants de l'institution, en consultation avec leurs conseillers juridiques.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Dans toute organisation, on peut s'attendre à ce qu'il y ait des divergences d'opinions. Certains employés peuvent avoir des opinions qui diffèrent passablement de la position officielle de leur employeur. Dans certaines institutions, il peut être dans l'intérêt public d'interdire aux employés d'utiliser le courriel de l'organisation, ou toute autre tribune, pour exprimer de telles opinions personnelles. Le cas échéant, les employés devraient en être informés et prévenus des conséquences possibles d'une infraction à cette politique.

Les institutions ne sont pas tenues de contraindre leurs employés au silence. Cependant, il y a un certain risque de semer la confusion dans l'esprit du public, si la position officielle d'une institution est remise en question ou contredite par un employé qui utilise le courriel de l'institution pour exprimer de telles opinions personnelles. Le risque est accru lorsque l'employé est un cadre supérieur de l'organisme ou un expert reconnu dans le champ d'activité de l'organisme.

Afin d'atténuer le risque de semer la confusion, tout en respectant le droit d'expression de ses employés, une institution peut exiger d'un employé dissident qu'il insère un « avis d'opinion personnelle » aux messages exprimant des points de vue contraires à sa position officielle. Un tel avis peut aider à limiter la responsabilité de l'organisme, dans l'éventualité où une personne subirait des préjudices parce qu'elle s'est fiée à l'opinion de l'employé plutôt qu'à la position officielle de l'institution.

Une telle mesure de sécurité ne suffira pas à limiter la responsabilité en toute circonstance. Les dirigeants de l'institution devraient consulter leurs conseillers juridiques afin d'évaluer les risques et de choisir la meilleure ligne de conduite et, s'il y a lieu, de rédiger le texte d'avis d'opinion personnelle.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : l'institution respecte le droit des employés à exprimer des opinions différentes de sa position officielle. Cependant, il y a un certain risque de semer la confusion dans l'esprit du public, si la position officielle d'une institution est remise en question ou contredite par un employé qui utilise le courriel de l'institution pour exprimer de telles opinions personnelles. Le risque est accru lorsque l'employé est un cadre supérieur de l'organisme ou un expert reconnu dans le champ d'activité de l'organisme.

Par conséquent, (nom de l'institution) exige d'un employé dissident qu'il insère un « avis d'opinion personnelle » aux messages exprimant des points de vue contraires à sa position officielle. Un tel avis peut aider à limiter la responsabilité de l'organisme dans l'éventualité où une personne subirait des préjudices parce qu'elle s'est fiée à l'opinion de l'employé plutôt qu'à la position officielle de l'institution. Cet avis doit être affiché sous le bloc-signature.

L'avis doit être affiché dans le format suivant (décrire ou fournir le format), et se lire comme suit : (fournir le texte exact de l'avis).

Avis d'opinion personnelle

Ce courriel, incluant toutes les pièces jointes, reflète l'opinion personnelle de l'expéditeur et ne représente pas l'opinion ou la position officielle de (nom de l'institution). (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du courrier et détruire tous les exemplaires de ce courriel. Merci.

2.11. Éviter d'utiliser la fonction « Répondre à tous »

Les utilisateurs qui reçoivent un courriel adressé à plusieurs personnes, ou en tant que membre d'une liste de diffusion, devraient éviter d'employer la fonction « Répondre à tous », sauf si la réponse présente un réel intérêt pour la majorité des personnes ayant reçu le message original.

Un des risques liés à l'utilisation de la fonction « Répondre à tous » est qu'en raison de la large diffusion du message, il peut être difficile de savoir exactement à qui revient la responsabilité d'agir.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

L'utilisation de la fonction « Répondre à tous » encombre inutilement, non seulement la boîte aux lettres des personnes qui ne souhaitent pas recevoir de réponse, mais aussi l'ensemble du système de courriel.

« Répondre à tous » peut également mettre dans l'embarras l'expéditeur ou une autre personne sur la liste de diffusion, si, par exemple, une information devant être partagée uniquement entre deux individus, est plutôt envoyée à toutes les personnes sur la liste.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les utilisateurs qui reçoivent un courriel adressé à plusieurs personnes, ou en tant que membre d'une liste de diffusion, sont informés de ne pas employer la fonction « Répondre à tous », sauf si la réponse présente un réel intérêt pour la majorité des personnes ayant reçu le message original.

3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles

La gestion des courriels exige l'établissement d'une méthode de description de l'information institutionnelle qui soit coordonnée et couvre l'ensemble des documents. Afin d'éviter une accumulation de courriels difficile à gérer, tous les messages et leurs pièces jointes, destinés à être conservés durant une période déterminée, doivent être bien classés, au moment opportun, selon un plan de classification à jour et global. Les boîtes aux lettres individuelles, les boîtes communes et les boîtes publiques devraient être gérées efficacement et de manière uniforme. La ligne « Objet » des courriels est souvent utilisée comme outil de recherche et doit donc refléter le plus fidèlement possible le contenu du message. Le système de classement des courriels devrait favoriser l'indexation, le stockage et la récupération des messages de manière structurée et efficace. Le système de classement devrait également préserver tout lien ou fil conducteur entre les courriels à l'intérieur d'une série, afin de pouvoir mettre en contexte chacun des messages.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Il y aura une description détaillée des documents de l'institution.
- Il y aura un ou des plans de classification détaillés et à jour, qui incluront les métadonnées.
- Les utilisateurs sauront où classer leurs courriels, ou ils seront guidés par des systèmes automatisés pour choisir l'endroit approprié.
- Les utilisateurs connaîtront et mettront en pratique des techniques simples pour faciliter la recherche et la récupération des documents.

3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels

Les courriels, à l'exception des messages éphémères et de ceux qui ne sont pas des documents organisationnels, devraient être retirés du système de courriel et placés dans un système séparé où ils seront classés selon un plan de classification approuvé par l'institution. Les courriels devraient être indexés et conservés pour être utilisés par l'institution, jusqu'au moment de leur élimination prévue au calendrier de conservation ou de leur archivage permanent. Le dépôt d'archives devra aussi être structuré et indexé pour assurer un repérage efficace.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les tribunaux canadiens ont adopté une approche reconnue selon laquelle un système de classement de documents appartenant à une des parties impliquées dans un litige devrait être structuré et indexé de manière à en faciliter l'utilisation par l'autre partie.

Repérer une preuve documentaire peut être extrêmement long, et une des parties au litige pourrait argumenter que les sommes à investir pour produire ces documents en cour sont trop élevées. Les tribunaux mettront en balance le coût de ces recherches et les avantages qu'il y aurait à pouvoir consulter ces preuves. Cependant, les tribunaux n'apprécient pas en général lorsqu'ils constatent que la majeure partie des coûts est due au fait que le système de classement est mal structuré.

Il ne faut jamais sous-estimer le coût de la découverte électronique. Dans un litige important, impliquant une grande institution, les frais peuvent s'élever à plusieurs centaines de milliers de dollars, et même à plusieurs millions. Certains défendeurs préfèrent un arrangement à l'amiable, non pas comme une admission de culpabilité, mais parce qu'un tel règlement s'avère moins dispendieux que de rassembler les preuves documentaires nécessaires à leur défense.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : un système de classement des courriels efficace et bien structuré sera tenu à jour. Les dirigeants et gestionnaires à tous les niveaux hiérarchiques devront travailler en étroite collaboration avec le gestionnaire de l'information pour (concevoir, perfectionner, développer) le système de classement de l'institution, afin de garantir que les courriels soient classifiés, classés et stockés de façon à pouvoir les retrouver facilement au besoin. Tous les utilisateurs devront gérer efficacement leurs courriels, supprimer ceux qui ne sont pas des documents organisationnels dès qu'ils ne sont plus utiles, classifier et classer fréquemment leurs courriels, et se conformer aux règles du système de classement en vigueur.



3.2. Déterminer où classer la copie « officielle »

Un plan de classification et un dépôt devraient être établis pour stocker les courriels reçus et envoyés qui sont considérés comme des documents gouvernementaux ou de l'information gouvernementale.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Plus il existe d'exemplaires d'un courriel, plus il est difficile de déterminer la copie « officielle ».

Idéalement, il ne devrait y avoir qu'un seul exemplaire d'un courriel, outre bien sûr la copie de sécurité. Cela n'est pas toujours possible, actuellement, compte tenu de la technologie disponible et d'autres considérations. Lorsqu'il existe plusieurs copies d'un courriel, de ses métadonnées et pièces jointes, il est important de fournir aux utilisateurs des règles claires leur permettant d'identifier, parmi toutes les copies, celle qui doit être considérée comme la copie officielle, et de savoir où la classer.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution mettra en place un plan de classification et un dépôt pour le stockage de la copie officielle des courriels considérés comme de l'information ou des documents gouvernementaux, de la manière suivante : (fournir une brève description du plan de classification et de la façon de placer les courriels dans le dépôt approprié / ou fournir un lien vers le document officiel qui contient cette information).

Le dépôt approprié pour le stockage des fichiers de courriels est organisé selon le contenu et la classification des documents, et non selon leur support.

3.3. Conserver les métadonnées associées aux courriels

Les métadonnées associées à un courriel devraient être conservées, tel que spécifié dans le document NCTTI 39 : Normes de l'information et de la technologie du Conseil du Trésor.



- Partie 1: Norme des métadonnées du Gouvernement en direct

(Source : http://www.tbs-sct.gc.ca/its-nit/standards/tbits39/crit391_fra.asp)

- Partie 2 : Norme du vocabulaire contrôlé

(Source : http://www.tbs-sct.gc.ca/cio-dpi/pols_fra.asp#IT)

La norme NCTTI 39 - Partie 1 – Norme des métadonnées du Gouvernement en direct, a adopté le *Dublin Core*, tel que décrit à l'adresse <http://www.dublincore.org/> comme principale norme de métadonnées pour la découverte des ressources. Les métadonnées sont essentielles pour atteindre les objectifs de navigation, de recherche, de partage de l'information et d'interopérabilité du Gouvernement en direct.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Sans les métadonnées, il est impossible de prouver l'authenticité, l'intégrité et la fiabilité des courriels, et le document électronique ne peut pas être considéré comme un document organisationnel. Les métadonnées aident à relier les courriels entre eux ou à d'autres informations, comme il est souvent nécessaire de le faire pour répondre à une demande d'accès à l'information, lors d'un audit ou d'une action en justice. Les métadonnées peuvent contenir plusieurs types d'informations.

- L'information de référence sert à identifier de façon unique un message.
- L'information sur le contenu précise l'objet du message.
- L'information de contexte documente les relations avec d'autres documents ou d'autres informations.
- L'information de fixité (indicateurs d'authenticité) documente les mécanismes de vérification de l'intégrité des données et les clés de validation pour en garantir l'authenticité.

Les métadonnées précisent où et quand le courriel a été créé, par qui, à qui il a été envoyé, à quel endroit il est conservé, comment il est formaté, quand il a été lu, etc. Elles peuvent aussi documenter les différentes procédures de migration appliquées à ce message durant une longue période de conservation.

Outre le document NCTTI 39 – Normes de l'information et de la technologie du Conseil du Trésor, les spécialistes en gestion de l'information voudront peut-être consulter les publications



suivantes afin de déterminer précisément quels éléments de métadonnées utiliser pour faciliter la gestion des courriels et de leurs pièces jointes dans leurs institutions respectives.

- Norme de métadonnées de la gestion des documents du gouvernement du Canada / Secrétariat du Conseil du Trésor. Groupe de travail du Gouvernement en direct sur les métadonnées. Sous-groupe sur la gestion des documents, février 2006 (<http://www.collectionscanada.gc.ca/information-management/002/007002-5001-f.html>)
- Gouvernement du Canada. Gestion de la correspondance de la haute direction. Profil d'application de métadonnées / Bibliothèque et Archives Canada, mars 2006 (<http://www.collectionscanada.gc.ca/information-management/002/007002-5003-f.html>)
- Profil d'application du Dublin Core pour la découverte des ressources Web au gouvernement du Canada / Secrétariat du Conseil du Trésor. Normes de l'information et interopérabilité, mars 2006. (http://www.tbs-sct.gc.ca/im-gi/meta/profil/profil00_fra.asp)
- Lignes directrices relatives à la mise en place des métadonnées pour la découverte des ressources Web du gouvernement du Canada, 5^e édition / Secrétariat du Conseil du Trésor. Groupe de travail sur les métadonnées du Gouvernement en direct. Sous-groupe de la formation, décembre 2006 (http://www.tbs-sct.gc.ca/im-gi/mwg-gtm/ts-sf/docs/2006/metaweb/metaweb00_fra.asp)
- De plus, on pourra consulter une récente mise à jour du Dublin Core, résultat des travaux réalisés au cours des dernières années sur le modèle de résumé selon le Dublin Core et sur les termes reliés aux métadonnées du DCMI (<http://dublincore.org/documents/dcmi-terms/>) [en anglais seulement].

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les métadonnées associées à un courriel seront conservées et protégées dans la même mesure et pour la même période de temps que le courriel lui-même.

Essentiellement, les courriels sont des données électroniques. Les métadonnées sont des données à propos des données. La plupart des métadonnées associées aux courriels agissent « en coulisse » et sont invisibles aux utilisateurs. Les métadonnées servent à identifier un message, de telle manière qu'il ne puisse être confondu avec aucun autre. Les métadonnées précisent l'objet du message, les pièces qui y sont jointes et peuvent faire le lien avec d'autres courriels créés ou reçus par l'utilisateur dans une direction, une division, un programme, un projet ou un groupe d'utilisateurs. Les métadonnées peuvent indiquer si un document a été modifié ou non, et le cas échéant, par qui, ou à partir de quel poste de travail.

Les métadonnées précisent où et quand un courriel a été créé, par qui, à qui il a été envoyé, où il est conservé, comment il est formaté, etc. Elles peuvent aussi documenter les différentes procédures de migration appliquées à ce message durant une longue période de conservation.

Les métadonnées sont essentielles pour établir l'admissibilité en preuve des courriels et leur crédibilité lors d'un audit ou d'une action en justice.



3.4. Classifier et classer les courriels systématiquement et fréquemment

Les courriels devraient être classifiés et classés systématiquement et régulièrement, à une fréquence qui convient à la nature des activités de l'institution (p. ex., une fois par jour), et conformément au plan de classification adopté par l'institution. Les courriels devraient ensuite être transférés dans un dépôt de données désigné par l'institution.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Tous les courriels et leurs pièces jointes destinés à être conservés durant une période déterminée doivent être adéquatement classifiés et classés, afin d'en faciliter le repérage, la récupération, l'utilisation et la diffusion à une date ultérieure.

Certains plans de classification sont basés sur les sujets (ex. : transport aérien, TPS, sites historiques, parcs, contrats de location d'immeubles, traités, etc.). Depuis quelque temps, on a tendance à adopter plutôt une classification selon les fonctions (ex. : mandat, ministère, direction, programme, projet, etc.), et, à l'intérieur des fonctions, selon les sujets.

En ce qui concerne la fréquence à laquelle les courriels devraient être classés, il n'existe pas d'intervalle type, applicable à tous les organismes et à tous les employés, contractuels ou autres utilisateurs. Certains experts en la matière recommandent de classer les courriels immédiatement après les avoir lus, alors que le contenu est encore frais à l'esprit du lecteur.

Plusieurs facteurs doivent être pris en considération, par exemple, le besoin pour les membres d'un groupe de travail de partager l'information contenue dans les courriels, ou la quantité de courriels que reçoit habituellement un utilisateur. Il peut aussi y avoir des facteurs organisationnels liés aux activités de l'institution, ou à l'un ou l'autre de ses programmes ou projets.

Il appartient à l'institution de déterminer ce qui constitue une fréquence convenable pour classer les courriels; celle-ci peut même varier selon les groupes ou les individus à l'intérieur de l'institution.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution utilise un système (basé sur les fonctions, basé sur les sujets, autre) pour classer et classer ses documents et informations.

Choisir une des deux options suivantes :

Option 1. Cette institution utilise un système de gestion des documents électroniques qui limite automatiquement le nombre d'endroits où un courriel peut être classé. L'utilisateur disposera habituellement d'un nombre restreint d'endroits où il peut classer ses informations, selon le poste qu'il occupe et les programmes ou projets auxquels il participe dans le cadre de son emploi. Cependant, la décision finale concernant le classement de ses documents appartient toujours à l'utilisateur. Le système offre des options de classement parmi lesquelles l'employé peut choisir celle qu'il juge la plus appropriée.

Option 2. Cette institution n'utilise pas de système de gestion des documents électroniques qui limite automatiquement le nombre d'endroits où un courriel peut être classé. L'utilisateur doit décider par lui-même où classer ses courriels et pièces jointes. Les utilisateurs devraient demander à leurs gestionnaires de leur fournir une liste de dossiers où ces documents devraient être classés.

3.5. Gérer le stockage en ligne temporaire des courriels

Un système de courriel devrait être en mesure de traiter les messages reçus et envoyés, leurs métadonnées et pièces jointes, et de les stocker temporairement en ligne (dans le système lui-même), jusqu'à ce qu'ils soient supprimés ou déplacés manuellement. Les dossiers devraient ensuite être rangés, à intervalles appropriés, dans une zone de stockage de longue durée, par l'utilisateur ou l'administrateur de système, ou grâce à un quelconque mécanisme automatisé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les logiciels d'application en gestion des courriels voient leur performance diminuer si la mémoire du système est utilisée à pleine capacité ou presque. Il est donc très important de déplacer les courriels vers un dépôt de données ou une zone de stockage où ils ne réduiront pas la performance du système.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : une seule copie des courriels, de leurs métadonnées et pièces jointes sera stockée dans une base de données institutionnelle.

Les courriels sont reçus ou créés à l'aide des logiciels de l'institution (Lotus, Ms Outlook, ou autre). Les courriels, métadonnées et pièces jointes sont automatiquement transférés dans un dépôt central géré par (nom de l'institution). Une fois le courriel transféré, l'expéditeur et tous les destinataires peuvent le consulter, comme s'il était stocké en ligne.

Veuillez noter que si le nombre de courriels dans le compte d'un utilisateur excède la limite de taille raisonnable pour un dossier ou la limite de temps, les administrateurs de systèmes devraient en aviser le gestionnaire de l'information et le gestionnaire responsable de cet utilisateur. Cependant, un administrateur de système ne doit pas supprimer les messages stockés en ligne – même pas ceux qui excèdent la limite de taille prédéterminée d'un dossier ou la limite de temps – à moins que le gestionnaire de l'information et le gestionnaire de l'utilisateur n'autorisent tous les deux cette suppression.

3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels

Une boîte aux lettres commune ne devrait être créée qu'à une seule fin et n'avoir qu'un seul propriétaire, lequel fixera des règles bien précises à l'intention des autres personnes qui y ont accès.

Les courriels qui ne correspondent pas à l'objectif de la boîte aux lettres ne devraient pas y être stockés. Il peut s'avérer nécessaire d'attribuer différents niveaux d'accès aux utilisateurs d'une boîte aux lettres commune ou d'un dossier, selon leur rôle ou leur responsabilité.

Les boîtes aux lettres publiques ne devraient être utilisées qu'à une seule fin ou à une fin restreinte et devraient être gérées par un seul propriétaire qui en établit les règles d'accès.

Les boîtes aux lettres individuelles peuvent aussi être mises en commun, jusqu'à un certain point, avec un nombre restreint de personnes faisant partie du groupe de travail de l'utilisateur.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------



Justification

Les boîtes aux lettres communes sont conçues pour offrir un point de contact unique pour un service en particulier, par exemple la réservation de salles de réunion, le dépannage informatique ou la réponse à diverses questions. N'importe qui peut contacter une boîte aux lettres commune, mais seul un nombre restreint de personnes est autorisé à lire les courriels qui lui sont adressés et à y répondre.

Dans le cas d'un service de dépannage, l'un ou l'autre des spécialistes autorisés peuvent ouvrir le message et décider ce qu'il y a à faire. Si un employé est en congé de maladie ou en vacances, le courriel sera tout de même consulté par une personne autorisée qui y donnera suite. Un groupe de fournisseurs de services peut utiliser une boîte aux lettres commune pour consulter une demande de service et y répondre.

Une boîte aux lettres individuelle peut également être mise en commun. Ainsi, tout dirigeant peut confier à un adjoint la tâche de consulter et de trier les courriels qui lui sont adressés. De même, un utilisateur peut permettre aux membres de son groupe de travail ou de son équipe de consulter sa boîte aux lettres, afin de garantir qu'aucune information essentielle ne soit échappée en son absence.

Par défaut, une boîte aux lettres publique est accessible à tous. Cependant, si l'on se fie aux meilleures pratiques en vigueur dans d'autres administrations gouvernementales, il est préférable qu'une telle boîte aux lettres soit utilisée par un plus petit groupe d'individus, en général moins de 24. Habituellement, le propriétaire d'une boîte aux lettres détermine quelles sont les personnes les plus susceptibles d'apporter une contribution à la discussion et les invite à y participer.

Une boîte aux lettres publique est une communauté de personnes partageant un même intérêt ou centrées sur un même sujet. Les membres de cette communauté peuvent envoyer un courriel posant une question à l'ensemble du groupe, et tout membre est libre d'y répondre. Il arrive souvent qu'un courriel adressé au groupe engendre une série de commentaires, de clarifications ou de questions additionnelles qui s'enchaînent comme le fil d'une conversation.

Normalement, les courriels ne peuvent être supprimés d'une boîte aux lettres publique à moins d'une autorisation spéciale.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : une boîte aux lettres commune (doit / devrait) avoir un seul objectif ou un objectif limité, et un seul propriétaire, lequel (doit / devrait) établir des règles très précises.

- L'objectif de la boîte aux lettres (réservation de salles de réunion, réservation d'équipements, dépannage informatique, etc.)
- Comment identifier un courriel auquel on a répondu, et quelle a été cette réponse
- Comment déterminer le suivi à apporter, s'il y a lieu
- Qui sont les membres du groupe et quel est leur niveau d'accès (lire, répondre, marquer, classer, stocker, supprimer)
- Qui devrait répondre à quel message
- Quels types de courriels doivent être considérés comme des documents organisationnels
- Où les messages et leurs réponses doivent être stockés (dans un seul dossier ou dans un petit nombre de dossiers)
- Quand supprimer un courriel de la boîte aux lettres

Le propriétaire de la boîte aux lettres et les membres du groupe qui la partagent ont certaines responsabilités en commun.

- Tous ceux qui ont accès à la boîte aux lettres commune doivent respecter les règles établies.
- Tous ceux qui ont accès à la boîte aux lettres commune partagent la responsabilité d'identifier les courriels qui devraient être conservés en tant que document organisationnel.
- Tous ceux qui ont accès à la boîte aux lettres commune sont responsables de supprimer les messages éphémères.

L'accès à une boîte aux lettres commune devrait être limité aux personnes qualifiées pour répondre aux questions qui lui seront adressées.

Les utilisateurs qui voudraient poser des questions ou adresser des demandes par courriel à une boîte commune devront connaître l'adresse de cette boîte et son objectif. L'adresse devrait être facile à trouver dans l'annuaire de courriel de l'institution, mais elle peut aussi être diffusée via un site web ou un écran d'ouverture de session, un courriel en multidiffusion, des affiches, des autocollants ou des dépliants placés dans le hall d'entrée d'un édifice ou dans certains bureaux.

Une boîte aux lettres individuelle peut aussi être mise en commun en autorisant des représentants d'un groupe de travail ou d'une équipe à consulter les courriels du propriétaire de la boîte, en son absence, et à leur donner suite. D'autres droits d'accès peuvent être accordés dans certaines circonstances.

- Si le gestionnaire de l'information a été consulté et s'il est d'accord.
- Si le responsable de la sécurité a été consulté et s'il est d'accord que ces droits ne représentent aucune menace à la sécurité ou la confidentialité.

Une boîte aux lettres publique (doit / devrait) avoir un seul objectif ou un objectif limité et un seul propriétaire, lequel doit établir des règles très précises.

- L'objectif de la boîte aux lettres; cet objectif (est / se limite à) (sujet de discussion ou champ d'intérêt et sous-thèmes associés)
- Comment identifier un courriel auquel on a répondu, et quelle a été cette réponse.
- Comment déterminer le suivi à apporter, s'il y a lieu
- Qui sont les membres du groupe et quel est leur niveau d'accès (lire, répondre)
- Combien de temps un message devrait demeurer dans la boîte aux lettres avant d'être rangé ou supprimé
- Combien de dossiers seront utilisés, et ce qu'ils contiendront

Le propriétaire d'une boîte aux lettres publique est responsable de gérer les documents et l'information qu'elle contient.



- Identifier quels courriels sont considérés comme des documents organisationnels
- Déterminer où les courriels et leurs réponses doivent être classés et stockés (dans quels dossiers les placer)
- S'assurer que le système de classement d'une boîte aux lettres publique est conforme aux pratiques de l'institution
- S'assurer que le système de classement d'une boîte aux lettres publique respecte les règles de l'institution en matière d'attribution des noms de dossiers
- Classifier et stocker les messages et leurs réponses
- Veiller à ce que les courriels dans une boîte aux lettres publique soient protégés et « inviolables »
- Supprimer de la boîte aux lettres les courriels non pertinents ou éphémères
- Informer un expéditeur qu'un courriel non pertinent a été supprimé, et en donner la raison
- Agir comme modérateur, afin que la discussion menée via la boîte aux lettres publique ne s'écarte pas du sujet
- Fermer la boîte aux lettres publique une fois son objectif atteint

Le propriétaire d'une boîte aux lettres et ceux qui la partagent ont certaines responsabilités en commun. Tous ceux qui ont accès à une boîte aux lettres commune doivent respecter les règles établies. Un courriel qui a contribué de façon importante à une discussion devrait être conservé à titre de document organisationnel, avec les conclusions de la discussion. Les courriels échangés via une boîte aux lettres publique fournissent le contexte dans lequel une décision finale a été prise. Ils doivent donc être conservés pour rendre compte du processus décisionnel.

3.7. Limiter le contenu des courriels à un seul sujet

Les utilisateurs ne devraient traiter que d'un seul sujet par courriel.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

À l'heure actuelle, le courriel est le type de preuve documentaire le plus souvent demandé par les cours de justice. Les tribunaux s'attendent à ce que les parties à un litige fournissent toutes les preuves pertinentes, mais uniquement des preuves pertinentes. S'il est produit en preuve, un courriel traitant de plus d'un sujet obligera la cour à examiner des informations qui ne sont pas pertinentes au litige.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : les courriels ne devraient traiter que d'un seul sujet, afin d'en faciliter le classement et la recherche.

3.8. Décrire l'objet d'un courriel en termes clairs et significatifs

Les utilisateurs devraient décrire l'objet de leurs courriels en termes significatifs, à l'aide de mots clés pouvant servir lors d'une recherche électronique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

À l'heure actuelle, le courriel est le type de preuve documentaire le plus souvent demandé par les cours de justice. Les tribunaux s'attendent à ce que les parties à un litige fournissent toutes les preuves pertinentes, mais uniquement des preuves pertinentes. La méthode privilégiée pour repérer l'information électronique telle que les courriels, consiste à effectuer diverses formes de recherche électronique. La recherche d'informations pertinentes est souvent faite dans les lignes « Objet » des courriels. Cette méthode est beaucoup plus rapide et efficace que la recherche dans le contenu des messages.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les utilisateurs devraient décrire l'objet de leurs courriels en des termes significatifs, à l'aide de mots clés pouvant servir lors d'une recherche électronique visant à repérer des documents sur un sujet en particulier.

3.9. Prévoir un système d'indexation des courriels

Les institutions devraient prévoir une indexation des courriels.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Il n'est pas très utile de conserver une énorme quantité de courriels s'il n'existe aucun moyen efficace d'y repérer de l'information. Il y a deux façons d'indexer les courriels.

1. Il existe des applications permettant d'effectuer une indexation plein texte des courriels; cette solution peut convenir à un certain nombre d'institutions. Cependant, ces logiciels sont plutôt dispendieux et doivent être passablement adaptés pour pouvoir trier les courriels dans un plan de classification préétabli. Sans cette adaptation, les logiciels créeront tout simplement un autre plan de classification qui correspondra peu ou pas au mode de fonctionnement de l'institution.
2. Une autre méthode d'indexation des courriels consiste à les classer selon un plan de classification préétabli, à l'aide d'un vocabulaire contrôlé.

Le vocabulaire contrôlé restreint le choix des termes de classification. Par exemple, un courriel créé par la direction des ressources humaines d'un ministère devra être classifié sous Direction des ressources humaines, et non sous Ressources humaines ou Personnel ou RH. Les métadonnées peuvent aussi, dans une certaine mesure, servir à la classification. Ainsi, à la simple ouverture d'une session à l'écran, un utilisateur révèle automatiquement pour quel ministère, organisme ou programme il travaille.

Normalement, il faudra aussi déterminer le sujet de classification du courriel – à ne pas confondre avec la ligne Objet du message. Par exemple, la ligne Objet d'un message pourrait être « Calendrier de formation », mais cela ne signifie nécessairement que le courriel sera classifié sous ces termes. Certains systèmes peuvent être configurés pour inciter l'utilisateur à sauvegarder le message; ils peuvent aussi être configurés pour offrir à l'utilisateur un choix restreint de sujets. Prenons l'exemple d'un concepteur de formation à l'emploi de la Direction des ressources humaines qui travaille sur trois projets différents. Un de ces projets a pour titre « Formation en gestion des courriels »; c'est peut-être sous ce titre qu'il convient de classer le message intitulé « Calendrier de formation ».

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : les courriels seront indexés à l'aide d'un (vocabulaire contrôlé / plan de classification informatisé).

Exemple(s):

(Fournir des exemples de vocabulaires contrôlés convenant à l'institution, et en décrire les implications).

3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (*threading*)

Les institutions devraient pouvoir suivre le fil conducteur qui relie les courriels entre eux. Le *threading* est un mécanisme par lequel un système de gestion de l'information peut suivre à la trace les relations existant entre des courriels, leurs métadonnées et pièces jointes, à l'intérieur d'une suite de courriels.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Dans un fil conducteur, il doit y avoir un courriel initial, suivi d'une séquence de réponses. Le fil peut contenir des courriels sous forme de questions et réponses, de points de vue exprimés lors d'une discussion ou de processus décisionnel. Lors d'un audit ou d'une action en justice, on exige souvent des preuves concernant une décision en particulier, ainsi que l'ensemble de la correspondance ayant entraîné cette décision. Par conséquent, il faut être en mesure de conserver le fil reliant entre eux une suite de courriels. Il faut pouvoir identifier et repérer tous les courriels pertinents qui sont reliés par un tel fil, et préserver l'ordre des messages.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les fils conducteurs reliant les courriels entre eux à l'intérieur d'une suite seront préservés. Une telle suite peut comprendre un message initial suivi d'une séquence de réponses reliées à une même question, de points de vue exprimés dans le cadre d'une discussion ou d'un processus décisionnel.

4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels

L'utilisation du courriel devrait être réservée à des usages appropriés et non à la transmission d'informations sensibles, protégées ou secrètes. Les journaux d'exploitation permettent de suivre à la trace l'utilisation des courriels et de préparer des rapports en conséquence, ceci afin de documenter le respect des politiques et procédures en vigueur, tant au niveau individuel que collectif. Le courriel est devenu une des formes de preuve les plus fréquemment utilisées par les tribunaux; les institutions doivent donc, en tout temps, être en mesure de communiquer des preuves sous forme de courriel. La gestion des courriels doit permettre aux utilisateurs un accès pratique et au moment opportun à des informations contenues dans les courriels, conformément aux exigences légales et réglementaires. Il pourrait être instructif d'utiliser des cas réels ou fictifs pour éprouver et analyser la capacité de l'organisme à repérer et à produire des courriels en preuve, de manière fiable et économique, lorsqu'ils sont requis par un tribunal, lors d'un audit ou d'une demande d'accès à l'information en vertu de l'AIPRP.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Les utilisateurs auront accès, de manière pratique et en temps opportun, aux informations qu'ils sont autorisés à voir ou à utiliser, et sauront comment procéder.
- Les cas réels exigeant le repérage de courriels à des fins juridiques, d'audit ou de demande d'information en vertu de l'AIPRP seront surveillés et analysés de manière régulière, afin d'établir des critères de performance, d'évaluer les risques et d'identifier les améliorations à apporter à la gestion des courriels.
- Des « exercices de découverte » à partir de cas fictifs seront conçus et menés occasionnellement afin de diagnostiquer de manière contrôlée la capacité de l'organisme à repérer et à produire des courriels.
- Les leçons apprises au cours de ces exercices seront partagées et mises en pratique.



4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur

Il faut éviter d'utiliser le courriel pour transmettre des informations confidentielles, sensibles, protégées ou secrètes, sauf s'il existe une raison opérationnelle précise de le faire et s'il est possible de recourir à des systèmes sécurisés ou au chiffrement des données. Le cas échéant, les utilisateurs doivent se conformer aux politiques et lignes directrices institutionnelles et gouvernementales en la matière (voir aussi 5.1.5).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Une fois qu'un courriel a été transmis, son auteur en perd le contrôle. À moins que le message n'ait été chiffré, et même là, l'auteur ne peut pas savoir à qui ce courriel a été réexpédié, ni si une personne non autorisée a pu le lire à l'écran du destinataire, ni si quelqu'un a pu en prendre connaissance à sa sortie d'une imprimante.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : le courriel non sécurisé ne devrait pas être utilisé pour transmettre des informations sensibles, personnelles, protégées ou secrètes. La plupart des documents gouvernementaux peuvent être divulgués au public dans le cours des opérations régulières du gouvernement, à l'occasion de transactions diverses, de collaborations dans différents dossiers ou projets, etc. Normalement, ces informations sont partagées avec nos clients et nos partenaires. Une grande partie de cette information est aussi accessible au public grâce à la loi sur l'accès à l'information.

Cependant, certains types de documents ou d'informations sont de nature sensible et peuvent être classés « protégés » ou « secrets ». En raison de la perte inévitable de contrôle sur les courriels à partir du moment où ils sont expédiés, il est fortement conseillé de ne pas transmettre les informations suivantes par courriel :

- Renseignements personnels contenus dans les dossiers de ressources humaines
- Renseignements personnels contenus dans les dossiers de santé
- Secrets commerciaux
- Informations pouvant violer les droits à la protection de la vie privée



Les utilisateurs sont avisés, par la présente, qu'il est interdit d'utiliser un courriel non sécurisé pour transmettre les informations suivantes :

- Mots de passe et codes d'accès
- Documents à l'intention du cabinet
- Documents classés « protégés » ou « secrets »
- Informations pouvant représenter un risque à la sécurité publique si elles étaient vues par des personnes non autorisées

Ce type d'information peut tout de même être transmis par courriel, mais seulement dans certaines circonstances, par des personnes autorisées, et à condition d'employer une technologie de chiffrement et de l'équipement spécialisé. Ces autorisations doivent être obtenues auprès de (responsable de la sécurité). Si les autorisations en question sont accordées, l'administrateur de système devra configurer en conséquence le compte de courriel de l'utilisateur et lui fournir l'équipement approprié.

4.2. Utiliser les journaux d'exploitation pour créer une piste de vérification et veiller au respect des règles

Les journaux d'exploitation devraient être utilisés pour créer une piste de vérification et enregistrer chacune des opérations effectuées en rapport avec les courriels, dans un système de courriel ou autre dépôt de données.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Une piste de vérification constitue un des principaux moyens d'établir l'intégrité et l'authenticité de la preuve lors d'une action en justice ou d'une vérification quelconque.

Les journaux d'exploitation peuvent être utilisés pour créer une piste de vérification. Celle-ci est en fait l'enregistrement d'une séquence d'événements ou d'épisodes permettant de reconstituer l'activité qui a eu lieu dans un fichier électronique. Une piste de vérification peut être utilisée pour établir le statut juridique d'un courriel et en confirmer, ou en infirmer, l'intégrité ou l'authenticité.

Les pistes de vérification peuvent aussi être utilisées à titre de preuve lors d'enquêtes criminelles, notamment dans les cas de délits informatiques.



Les pistes de vérification peuvent aussi servir, de manière plus générale, à documenter, confirmer ou infirmer la fiabilité d'un système informatique, et à vérifier si les utilisateurs respectent les normes de sécurité en vigueur.

Les logiciels de courriel comportent habituellement des outils de vérification simples; il est également possible de se procurer des outils de vérification plus spécialisés auprès de divers fournisseurs.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante en matière de vérification : les journaux d'exploitation (créés grâce à des outils intégrés aux logiciels de courriel ou à des outils de vérification provenant de fournisseurs extérieurs) seront utilisés pour garantir l'authenticité, l'intégrité et la fiabilité des courriels, afin d'en établir l'admissibilité en preuve et donner plus de poids à cette preuve.

- Les journaux d'exploitation devraient dépister et enregistrer tous les épisodes, autorisés ou non, d'accès ou de tentatives d'accès, à un ou à des courriels, groupes de courriels, métadonnées ou pièces jointes.
- Les journaux devraient dépister et enregistrer tous les épisodes, réussis ou non, d'effacement ou de modification de courriels, de métadonnées ou de pièces jointes, que ces opérations aient été autorisées ou non.
- Les journaux devraient dépister et enregistrer la date et l'heure de chaque épisode, ainsi que le nom des intervenants ou, à défaut, le poste de travail où l'épisode a eu lieu.
- Les journaux devraient préciser où se trouve le fichier de courriel et où il est physiquement conservé.
- Les journaux devraient être utilisés pour documenter la fiabilité du système de courriel.
- Les journaux devraient permettre de surveiller le respect des Lignes directrices pour la gestion des courriels.
- Les journaux peuvent être générés automatiquement par le système ou à demande, et prendre diverses formes : journal des transactions, journal de sauvegarde, journal des erreurs et des défaillances, journal des pistes de vérification, etc.

4.3. Afficher les noms dans les en-têtes et les adresses de courriel

L'en-tête d'un courriel devrait afficher le nom de l'auteur (De) et celui du destinataire (À), conformément aux normes gouvernementales relatives aux métadonnées.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

Les noms propres facilitent notre identification et celle des autres. Cependant, il peut arriver, au sein d'une grande institution, que deux personnes portent le même nom ou des noms très similaires. Il faudra trouver une façon de bien les distinguer.

Il y aura inévitablement des cas où l'ordre de présentation des noms ou des initiales, ou une règle quelconque de raccourci des noms, donnera un résultat inapproprié qui pourrait paraître étrange, ridicule ou même insultant dans une autre langue.

La plupart des organismes choisissent d'indiquer au complet le nom et le prénom de l'expéditeur et du destinataire dans l'en-tête du courriel, à condition que le nom et le prénom du destinataire soient effectivement connus de l'expéditeur ou bien enregistrés dans le système.

On observe davantage de variations dans les adresses de courriel. Certains organismes utilisent le nom au complet, avec à l'occasion une initiale supplémentaire. D'autres ont pris l'habitude de raccourcir ou de tronquer les noms. L'utilisation de noms raccourcis ou de surnoms n'est pas recommandée; en effet, en cas d'audit ou d'action en justice, cela peut avoir pour effet de compliquer l'identification de l'expéditeur, du destinataire ou du récipiendaire. D'une manière générale, il est préférable de respecter le choix des personnes elles-mêmes. Par exemple, Patrick McGuire préfère peut-être se faire appeler « paddy.mcguire » et Patrick Loubert préfère peut-être « pat.loubert », parce que c'est ainsi qu'ils se présentent habituellement ou qu'ils souhaitent qu'on s'adresse à eux.

En vertu de la politique de normalisation des sites Internet (NSI), « la résolution des conflits d'affectation des noms dans la partie locale (la partie se trouvant avant le symbole @) est laissée à la discrétion de l'administrateur de courrier électronique de l'institution. La préférence devrait être accordée à l'insertion de l'initiale de l'employé dans la partie locale. Dans des circonstances exceptionnelles, il est possible d'adopter une autre règle d'affectation de noms pour répondre à des objectifs liés à la sécurité ».

Des exceptions peuvent être tolérées dans les cas où, par convention culturelle, le nom de famille précède le prénom.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter



l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : d'une manière générale, on utilisera comme identifiant le nom que la personne elle-même préfère. Ainsi, Patrick McGuire pourrait être exprimé par « paddy.mcguire » et Patrick Loubert par « pat.loubert », si c'est de cette manière qu'ils se présentent habituellement ou qu'ils souhaitent qu'on s'adresse à eux.

L'utilisation de noms raccourcis ou de surnoms n'est pas recommandée; en effet, en cas d'audit ou d'action en justice, cela peut avoir pour effet de compliquer l'identification de l'expéditeur, du destinataire ou du récipiendaire.

Il peut y avoir des exceptions à cette règle générale lorsque des questions d'ordre personnel ou de sécurité nationale entrent en ligne de compte. On pourra aussi faire des exceptions dans les cas où, par convention culturelle, le nom de famille précède le prénom, ou quand l'ordre de présentation du nom, du prénom, des initiales ou du surnom donne un résultat inapproprié.

4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique

Les systèmes de stockage et de classement des courriels, incluant les systèmes en ligne et les systèmes de stockage de proximité, qu'ils soient à court ou à long terme, doivent permettre aux chercheurs d'identifier, de divulguer ou de produire rapidement des courriels, ainsi que leurs métadonnées et pièces jointes, lors d'une action en justice, d'un audit ou d'une demande en vertu de l'AIPRP. Afin de faciliter la récupération efficiente d'un document à des fins de divulgation, les courriels devraient être classés conformément à un plan de classification institutionnel approuvé (voir aussi la troisième section des Lignes directrices et les recommandations qui s'y trouvent).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

La « découverte » est le processus au cours duquel chacune des parties impliquées dans une action en justice divulgue à l'autre partie toute la preuve pertinente qu'elle détient. Il est arrivé

que certains juges rendent des décisions défavorables à l'encontre de parties qui ne pouvaient produire la preuve en leur possession.

Les règles de procédure civile et la jurisprudence ont clairement élargi aux documents électroniques l'obligation de divulgation et de production de documents en cour. Les parties doivent identifier les données repérables et récupérables, et divulguer entièrement aux autres parties les documents électroniques en leur possession, contrôle ou pouvoir, dans la mesure où ils sont pertinents au litige.

Un audit peut prendre plusieurs formes. Le Bureau du vérificateur général du Canada a le pouvoir de vérifier les systèmes de contrôle financier, les procédures organisationnelles, les programmes de subventions, la performance et même les mesures de sécurité. En fait, ce sont littéralement toutes les composantes des activités d'un organisme que le vérificateur peut, en théorie, examiner. Le vérificateur général est en droit de demander toute information probante jugée nécessaire dans le cadre d'un audit et les membres de la fonction publique ont l'obligation de répondre à ces demandes. Ceci inclut les courriels.

Les demandes d'accès à l'information peuvent aussi exiger la divulgation de courriels.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : (nom de l'institution) sera en tout temps préparé à répondre, aussi rapidement que possible, aux demandes de divulgation de preuves lors d'un audit, d'une action en justice ou d'une demande en vertu de l'AIPRP. Les systèmes de stockage et de classement de courriels, incluant les systèmes en ligne et les systèmes de stockage de proximité, qu'ils soient à court ou à long terme, doivent être conçus et tenus à jour de façon à ce qu'un chercheur puisse rapidement repérer, divulguer et produire des courriels pertinents (mais seulement ceux qui sont pertinents), ainsi que leurs métadonnées et pièces jointes, en format électronique.

4.5. Surveiller la performance des activités de découverte et de disposition des courriels

Les organismes devraient surveiller l'efficacité de leur performance en matière de découverte et de disposition des courriels. Ceci est nécessaire en vertu de plusieurs politiques du Secrétariat du Conseil du trésor, notamment la Politique sur la gestion de l'information, la Politique sur la surveillance active, la Politique d'évaluation et la Politique sur la vérification interne.



Des « exercices » devraient être menés régulièrement, que ce soit à partir de cas réels ou de cas simulés pour l'occasion. On en profitera alors pour concevoir et tester des mesures de performance, et évaluer l'efficacité et l'efficacé des procédures de découverte et de disposition des courriels.

Les observations résultant de ces exercices devraient être partagées et analysées sous forme de « leçons apprises », et mises à la disposition de toute personne impliquée dans la découverte ou la disposition des courriels, ou dans l'évaluation et l'amélioration des pratiques de l'institution en matière de gestion de l'information.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les règles de procédure civile et la jurisprudence ont clairement élargi aux documents électroniques l'obligation de divulgation et de production de documents en cour. Les parties doivent identifier les données repérables et récupérables, et divulguer entièrement aux autres parties les documents électroniques en leur possession, contrôle ou pouvoir, dans la mesure où ils sont pertinents au litige.

L'information peut être « découverte » en format électronique, même si elle a déjà été divulguée sur support papier.

Certaines informations doivent aussi être éliminées en vertu d'obligations légales, à l'expiration d'un délai de conservation prévu. En règle générale, il s'agit d'informations de nature personnelle. Lorsque de telles informations doivent être éliminées, l'institution doit détruire toutes les copies en sa possession, où qu'elles se trouvent, dans divers ordinateurs ou serveurs, sur des disques durs ou des bandes de sauvegarde; ces copies peuvent aussi être sous forme latente, mais récupérable.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : (nom de l'institution) sera en tout temps préparé à répondre, aussi rapidement que possible, aux demandes de divulgation de preuves de courriels lors d'un audit, d'une demande d'accès à l'information ou d'une action juridique.

Dans les cas où des documents sous contrôle de cette institution sont assujettis à un délai de conservation fixé par la loi, cette institution veillera, en vertu de sa politique, à repérer ces informations et à en disposer au moment opportun.

Afin de garantir que l'institution soit bien préparée à ces responsabilités, la performance des activités de découverte et de disposition sera examinée à l'occasion d'exercices (construits autour de cas réels ou fictifs) à intervalles réguliers. Par exemple, de tels exercices pourraient avoir lieu au moins une fois par année dans chaque direction générale, ou plus souvent si les résultats sont décevants.

Le but de ces exercices sera de déterminer l'efficacité de chaque direction générale et de l'organisme au complet, en matière de gestion des courriels. Les exercices seront autant d'occasions de vérifier la capacité de l'organisme à repérer, divulguer et produire rapidement des courriels pertinents (mais seulement ceux qui sont pertinents), ainsi que leurs métadonnées et pièces jointes.

Les exercices devront refléter des situations réelles ou fictives d'actions en justice, de procédures d'audit ou d'éliminations prévues au calendrier de conservation; ils devront inclure le repérage ou la récupération d'informations et de documents réels.

Sans être exhaustive, la liste qui suit identifie plusieurs critères de performance à considérer :

- Combien de temps a-t-il fallu pour repérer l'information?
- Combien de temps a-t-il fallu pour placer des ordres de retenue afin d'empêcher la destruction de documents prévue au calendrier de conservation?
- Est-ce que toutes les copies d'un fichier ont été retrouvées, y compris les copies latentes?
- L'exercice a-t-il permis de repérer des fichiers qui auraient dû être détruits?
- Les copies latentes de fichiers ont-elles été repérées?
- Est-ce qu'une copie de chaque fichier recherché a été repérée à l'endroit où elle devait normalement se trouver?
- Est-ce que les lignes Objet ont été utiles pour repérer les informations pertinentes?
- Est-ce que les listes de distribution ont été conservées?

L'évaluation de la performance durant un exercice vise à identifier des problèmes et des défis en matière de gestion des courriels; elle vise aussi à proposer, le cas échéant, des mesures pour améliorer le temps de réaction et l'efficacité.



5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés

Les institutions doivent veiller à ce que l'information possédant une valeur de conservation permanente pour le gouvernement du Canada ou pour les Canadiens puisse être utilisée, maintenant et dans les années futures. Les institutions devraient effectuer une évaluation des risques afin d'établir les délais de conservation appropriés à chaque type d'information. L'établissement de ces délais repose essentiellement sur le contenu des documents et non sur leur support physique ou sur la technologie utilisée pour les créer. Les utilisateurs du courriel devraient se référer au plan de classification et au calendrier de conservation de leur institution, afin de s'assurer que leurs messages soient classés au bon endroit et pour une période de temps appropriée.

Les documents essentiels doivent être sauvegardés. Ils devraient être protégés par des mesures de sécurité propres aux réseaux électroniques et des mesures de sécurité physiques. Il faut aussi en garantir la facilité d'utilisation, même s'ils sont chiffrés, malgré le temps qui passe et les changements technologiques. Il est essentiel de créer, tenir à jour et conserver une documentation du système de courriel et du système de stockage, afin de pouvoir récupérer les données après un sinistre, ou authentifier des courriels lors de demandes dans le cadre d'actions en justice, d'audits ou de l'AIPRP. Les organismes doivent aussi être capables de protéger leurs courriels contre toute divulgation, utilisation, disposition ou destruction inappropriées, et cela, en vertu des obligations découlant de lois et de politiques en vigueur. Il sera peut-être nécessaire, à l'occasion, d'appliquer un ordre de retenue, afin de retarder l'élimination de documents qui pourraient être requis à des fins juridiques.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Les informations contenues dans les courriels et possédant une valeur de conservation permanente pour le gouvernement du Canada ou pour les Canadiens pourront être utilisées, de manière fiable, maintenant et dans les années futures.
- Il sera possible de garantir la facilité d'utilisation des courriels, même s'ils sont chiffrés, malgré le temps qui passe et les changements technologiques.
- Les utilisateurs de courriel devront connaître les calendriers de conservation, lesquels seront appliqués correctement en fonction du contenu des courriels, ou automatiquement en fonction de la classification de ces courriels.



- Les courriels devront être protégés de manière fiable contre toute divulgation, utilisation, disposition ou destruction inappropriées, et cela, en vertu des obligations découlant de lois et de politiques en vigueur.

5.1. Éviter de procéder à des purges indiscriminées dans les systèmes de courriel

Les utilisateurs, tout comme les administrateurs de systèmes ou de réseaux, ne devraient jamais procéder à des purges périodiques et indiscriminées de messages dans les systèmes de courriel, qu'elles soient manuelles ou automatiques. La disposition ou l'élimination des courriels devrait toujours se faire conformément à un calendrier de conservation approuvé par l'institution, et non pas simplement quand la boîte aux lettres est « pleine » ou que les messages dépassent une limite de temps arbitraire.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Il peut paraître raisonnable, du point de vue des technologies de l'information, de vouloir réduire la pression sur les systèmes de courriel en éliminant automatiquement les messages qui dépassent une certaine date prédéterminée. Cependant, une telle approche n'a aucun sens en gestion de l'information.

L'élimination indiscriminée d'anciens courriels entraîne inévitablement la perte d'informations ou de documents gouvernementaux importants. De plus, la destruction non autorisée de documents constitue un délit en vertu de la Loi sur la Bibliothèque et les Archives du Canada et de quelques autres lois. La destruction indiscriminée d'informations pourrait empêcher l'organisme de produire des courriels en preuve quand cela lui sera demandé. De solides pratiques en gestion de l'information devraient plutôt être instaurées pour gérer les courriels, ce qui aurait pour effet de réduire le fardeau des serveurs et de permettre l'élimination des courriels en fonction des calendriers de conservation.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : les courriels et l'information associée doivent être gérés de manière organisée. Les utilisateurs doivent supprimer les courriels qui ne sont pas des documents organisationnels dès qu'ils ne sont plus utiles, classer et classer les messages, leurs métadonnées et pièces jointes, qui contiennent des informations ou des documents gouvernementaux, et les conserver durant une période de temps appropriée.

Il n'est pas acceptable, sous aucune considération, et pour qui que ce soit, de supprimer des messages, des métadonnées ou des pièces jointes simplement en fonction d'un âge limite arbitraire.

5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées

Afin de permettre à l'institution de poursuivre son travail, les systèmes et programmes de gestion des courriels devraient avoir la flexibilité nécessaire pour permettre au personnel autorisé d'avoir accès aux courriels d'un employé, lorsque cette personne est absente.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Outre la nécessité d'accéder à certaines informations à des fins juridiques, la principale raison justifiant de bonnes pratiques en gestion des courriels et de l'information en général, est d'en favoriser l'accès aux employés du gouvernement et au grand public. Il n'y aurait aucune raison de conserver et de protéger des courriels, s'il n'était jamais nécessaire de consulter des documents anciens pour des raisons internes, de satisfaire les besoins du public en matière d'information, de préserver des informations de nature historique ou de garantir l'imputabilité du gouvernement.

De temps à autre, un employé doit s'absenter du travail. Cela peut être assez perturbant si cette personne possède dans ses courriels des informations que d'autres employés autorisés devraient connaître pour effectuer leur propre travail. Afin de prévenir une telle situation, un employé pourrait autoriser une ou plusieurs autres personnes de son unité de travail à détenir un accès « en lecture seulement » à son compte de courriel.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : afin de ne pas interrompre la réalisation des activités de (nom de l'institution), les systèmes et programmes de gestion des courriels doivent avoir la flexibilité nécessaire pour permettre au personnel autorisé d'avoir accès aux courriels d'un employé, lorsque cette personne est absente.

Les utilisateurs sont informés, par la présente, qu'un des administrateurs de systèmes pourra, en tout temps, et pour toute raison valable, avoir accès au compte de courriel d'un utilisateur, afin de lire, copier, faire suivre, classer ou détruire un ou des messages, avec l'autorisation de l'une ou l'autre des personnes suivantes :

- L'utilisateur lui-même
- Le gestionnaire de l'utilisateur
- L'officier responsable de la sécurité de (nom de l'institution)
- Le conseiller juridique de (nom de l'institution)

Les raisons valables invoquées peuvent comprendre, notamment, la nécessité d'obtenir certaines informations du compte de courriel d'un utilisateur, en son absence, afin d'être en mesure de poursuivre un travail en cours ou de partager certaines informations critiques, le besoin de continuer de servir le public et la nécessité de disposer de certaines informations à titre de preuve lors d'une action en justice ou d'un audit. Un tel accès peut aussi être requis en cas d'enquête concernant une possible utilisation abusive du système de courriel.

Si un utilisateur expédie ou reçoit régulièrement des informations par courriel, et que d'autres personnes autorisées peuvent avoir besoin de ces informations, l'utilisateur peut autoriser un ou plusieurs collègues de son unité de travail à détenir un accès « en lecture seulement » à son compte de courriel.

5.3. Enlever le chiffrement avant de quitter une institution

Le chiffrement des messages et de leurs pièces jointes doit être enlevé avant que l'utilisateur ne quitte son emploi dans une institution.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Le chiffrement consiste à remplacer le texte d'un message ou de pièces jointes par un code que seuls les destinataires autorisés sont capables de déchiffrer afin de reconstituer le texte original. Les enfants connaissent bien le code, très simple, qui consiste à remplacer les lettres de l'alphabet par un chiffre (A = 1, B = 2, C = 3, etc.). Les technologies modernes de chiffrement utilisent des



codes infiniment plus complexes, mais elles peuvent chiffrer un message (c'est-à-dire appliquer le code) et le déchiffrer d'une simple pression d'un bouton.

L'utilisation du courriel n'est pas recommandée pour la transmission de messages et de pièces jointes qui contiennent de l'information sensible, protégée ou secrète. Cependant, dans certaines circonstances définies par la politique de sécurité et autorisées par la direction de l'institution, de telles informations peuvent être transmises, à condition d'être chiffrées au moyen d'un système de chiffrement approuvé par le gouvernement du Canada.

Voir : Politique de gestion de l'Infrastructure à clé publique au gouvernement du Canada
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_f.asp

Bibliothèque et Archives Canada déclare que :

Le chiffrement des données permet de sécuriser davantage les documents électroniques en mémoire ou lors de leur transmission. Il accroît la confidentialité du contenu d'un document et en restreint l'accès. Dans le cas des documents en mémoire, le chiffrement est semblable aux mesures de sécurité physique et ne fait donc pas partie du document comme tel.

Pendant la transmission d'un document, le chiffrement remplit la fonction d'une enveloppe de papier traditionnelle. Comme cette « enveloppe » ne fait pas partie intégrante du document et puisque traditionnellement les enveloppes ne sont pas jugées de valeur durable, les Archives nationales ne conserveront pas la version chiffrée des documents électroniques.

(Source : <http://www.collectionscanada.gc.ca/gestion-information/002/007002-3015-f.html>)

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante, conformément aux directives de Bibliothèque et Archives Canada : le chiffrement des courriels destinés à être archivés doit être enlevé. La capacité de lire un courriel chiffré et celle d'enlever le chiffrement doivent être maintenues tant que le chiffrement n'aura pas effectivement été enlevé, à un moment prévu durant la période de conservation du courriel ou à l'expiration de son délai de conservation, juste avant d'être versé à Bibliothèque et Archives Canada. Afin de soutenir cette politique, le chiffrement doit être retiré des messages courriels et des pièces jointes avant qu'un utilisateur quitte une institution.



5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada

Le chiffrement devrait être enlevé des courriels et de leurs pièces jointes avant leur transfert à Bibliothèque et Archives Canada. L'utilisateur devrait retirer lui-même le chiffrement du message, s'il travaille encore pour l'organisme. Autrement, c'est le gestionnaire des opérations responsable de la section de l'organisme où le message a été chiffré qui devrait enlever le chiffrement; dans ce cas, il est possible que soient requis l'avis d'un spécialiste en gestion de l'information et le soutien d'un administrateur de réseau ou de système. En l'absence de l'utilisateur et du gestionnaire des opérations, le spécialiste en gestion de l'information devrait avoir l'autorisation de décoder le message, avec l'aide d'un administrateur de réseau ou de système.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

Les messages chiffrés ne seront pas acceptés par Bibliothèque et Archives Canada

Voir la Politique de gestion de l'Infrastructure à clé publique au gouvernement du Canada (http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_f.asp)

Bibliothèque et Archives Canada déclare que :

Le chiffrement des données permet de sécuriser davantage les documents électroniques en mémoire ou lors de leur transmission. Il accroît la confidentialité du contenu d'un document et en restreint l'accès. Dans le cas des documents en mémoire, le chiffrement est semblable aux mesures de sécurité physique et ne fait donc pas partie du document comme tel.

Pendant la transmission d'un document, le chiffrement remplit la fonction d'une enveloppe de papier traditionnelle. Comme cette « enveloppe » ne fait pas partie intégrante du document et puisque traditionnellement les enveloppes ne sont pas jugées de valeur archivistique, les Archives nationales ne conserveront par la version chiffrée des documents électroniques.

(Source : <http://www.collectionscanada.gc.ca/gestion-information/002/007002-3015-f.html>)

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante, conformément aux directives de Bibliothèque et Archives Canada : le chiffrement des courriels destinés à être archivés doit être enlevé. La capacité de lire un courriel chiffré et celle d'enlever le chiffrement doivent être maintenues tant que le chiffrement n'aura pas effectivement été enlevé, à un moment prévu durant la période de conservation du courriel ou à l'expiration de son délai de conservation, juste avant d'être versé à Bibliothèque et Archives Canada.

5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel

Les programmes et les systèmes de courriel devraient s'appuyer sur des réseaux protégés par des technologies éprouvées, tels les coupe-feux, et une protection devrait être fournie contre les menaces suivantes (liste non exhaustive) :

- Accès non autorisé
- Virus, vers, chevaux de Troie, ActiveX et Applets Java
- Pourriels
- Mouchards, publiciels et fenêtres contextuelles
- Toute autre menace invasive qui pourrait apparaître

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les systèmes et programmes de courriel d'un organisme sont entièrement dépendants de leurs connexions à des réseaux. Ces réseaux doivent donc être protégés d'une foule de menaces, incluant les accès non autorisés.

Il est impossible de neutraliser entièrement toutes les menaces et de se prémunir contre tous les risques. Les mesures de protection doivent être proportionnelles aux menaces et aux risques potentiels.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter



l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les réseaux soutenant les systèmes et les programmes de courriel doivent être protégés contre les menaces, notamment les suivantes :

- Accès non autorisé
- Virus, vers, chevaux de Troie, ActiveX et Applets Java
- Pourriels
- Mouchards, publiciels et fenêtres contextuelles
- Toute autre menace pouvant apparaître

L'ampleur des mesures adoptées devrait être proportionnelle aux risques et menaces. Le (responsable de la sécurité) doit être consulté et une analyse des risques et des menaces doit être effectuée afin de déterminer les mesures de protection appropriées.

5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets

Les administrateurs de réseaux ou de systèmes devraient instaurer des systèmes de mots de passe et veiller à ce que les utilisateurs se conforment aux politiques concernant les mots de passe. Une première démarche consiste à protéger les mots de passe eux-mêmes. À cette fin, les administrateurs doivent changer les mots de passe par défaut installés par le fabricant du système d'exploitation ou du logiciel. Ces mots de passe par défaut sont bien connus des pirates informatiques, ce qui leur permet d'avoir accès aux centaines ou milliers de mots de passe en usage dans l'organisation.

Les utilisateurs devraient choisir des mots de passe difficiles à deviner – il faut éviter le nom de ses enfants, de son chien, de son équipe de sport favorite, de célébrités locales, etc. Les mots de passe devraient se conformer aux normes et caractéristiques établies par l'institution. Les utilisateurs devraient aussi garder secrets leurs mots de passe et les changer périodiquement.

Suggestions visant à améliorer la sécurité des mots de passe

Source : Manuel canadien de la sécurité des technologies de l'information – section 16.1.1 – Mots de passe

Disponible auprès du Centre de la sécurité des télécommunications Canada

Générateurs de mots de passe	Si les utilisateurs n'ont pas la possibilité de générer leur propre mot de passe, il leur est impossible de choisir des mots de passe faciles à mémoriser. Certains générateurs ne créent que des mots de passe ne comprenant aucun mot, mais étant prononçables pour pouvoir être mémorisés par les utilisateurs. Cependant, les utilisateurs ont tendance à écrire les mots de passe difficiles à mémoriser.
------------------------------	--

Phrases servant de mots de passe	L'utilisation d'une courte phrase au lieu d'un simple mot peut améliorer la résistance des mots de passe. La phrase est habituellement facile à
----------------------------------	---



Suggestions visant à améliorer la sécurité des mots de passe

Source : Manuel canadien de la sécurité des technologies de l'information – section 16.1.1 – Mots de passe

Disponible auprès du Centre de la sécurité des télécommunications Canada

	mémoriser et donne de bons résultats en matière de sécurité si les phrases évidentes sont évitées.
Nombre limité de tentatives d'entrer en communication	De nombreux systèmes d'exploitation peuvent être configurés pour effectuer un verrouillage après un certain nombre de tentatives d'entrer en communication infructueuses. Ce procédé permet de rendre les mots de passe impossibles à deviner.
Attributs de mot de passe	Les utilisateurs peuvent être priés, ou forcés par le système TI, de sélectionner des mots de passe 1) d'une certaine longueur minimale; 2) comprenant des caractères spéciaux; 3) n'ayant aucun rapport avec leur identification; 4) qui ne font pas partie d'un dictionnaire en ligne. Les mots de passe ainsi créés sont plus difficiles à deviner (mais ils ont plus tendance à être écrits).
Changement des mots de passe	Le changement régulier des mots de passe peut amoindrir les dommages causés par l'utilisation de mots de passe volés et rendre plus difficiles les attaques en force visant à pénétrer dans les systèmes TI. Il est cependant possible que des changements trop fréquents finissent par irriter les utilisateurs.
Protection technique du fichier du mot de passe	Le contrôle d'accès et le chiffrement unidirectionnel peuvent être utilisés pour protéger le fichier du mot de passe lui-même. Il est cependant indispensable de ne pas oublier que toutes les protections peuvent être annulées par des attaques suffisamment sophistiquées.

Source : <http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg-f.html>

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

Dans la littérature concernant la sécurité des technologies de l'information, un des risques souvent décrits est qu'une personne utilise le mot de passe d'une autre personne pour obtenir un accès non autorisé à des courriels, ou pour expédier des informations fausses ou nuisibles à partir du compte de cette personne; un tel geste peut causer un désagrément ou un préjudice, intentionnel ou non, à la personne en question, à l'organisme ou au destinataire. Ces risques peuvent être atténués grâce à la mise en place d'un système efficace de mots de passe.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les administrateurs de systèmes doivent mettre en place un système de mots de passe comprenant au minimum huit (8) caractères, dont au moins un doit être une lettre majuscule de l'alphabet romain, et au moins un doit être un chiffre.

L'utilisation d'autres caractères tels que @, #, \$, %, &, *, etc. dans des mots de passe n'est pas recommandée. Certains logiciels ne peuvent reconnaître que les mots de passe contenant des lettres ou des chiffres et ne reconnaîtront pas ces caractères spéciaux.

5.7. Protéger les systèmes contre les pertes ou les dommages

Les systèmes de courriels et les réseaux qui les soutiennent devraient être protégés contre les pertes ou les dommages pouvant provenir de plusieurs sources, dont les suivantes (liste non exhaustive) :

- Menaces physiques aux édifices et aux équipements informatiques
- Désastres naturels et menaces environnementales
- Défaillances des systèmes ou des équipements informatiques
- Vulnérabilité des supports
- Vulnérabilité des communications
- Absence ou perte de documentation
- Erreur humaine
- Autres menaces éventuelles pouvant émerger

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Enregistrer régulièrement une copie de sécurité est une chose, mais le local où se trouve le serveur est-il toujours fermé à clé? Ce local est-il situé au sous-sol d'un édifice exposé aux inondations? Si un feu se déclare dans ce local, est-ce que les extincteurs sont de type à protéger



(ou à détruire) les équipements ou les supports électroniques? Si un feu se déclare aux étages supérieurs, qu'est-ce qui empêchera l'eau de couler sur le serveur? Est-ce que les bandes de sauvegarde sont protégées des acariens et de la moisissure? Si le responsable du local où se trouve le serveur est soudainement dans l'impossibilité de remplir ses fonctions, la documentation requise pour prendre la relève est-elle disponible? Est-ce que cette documentation indique précisément au remplaçant où se trouvent les bandes de sauvegarde? Existe-t-il une copie de sécurité de cette documentation? Est-elle conservée dans un autre endroit?

Il est essentiel d'examiner l'ensemble des menaces, d'évaluer les risques et de prendre les mesures nécessaires pour en atténuer les impacts négatifs potentiels.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les systèmes soutenant le courriel devraient être protégés contre une foule de menaces qui pourraient causer des pertes ou des dommages.

- Menaces physiques aux édifices et aux équipements informatiques
- Désastres naturels et menaces environnementales
- Défaillances des systèmes ou des équipements informatiques
- Vulnérabilité des supports
- Vulnérabilité des communications
- Absence ou perte de documentation
- Erreur humaine

5.8. Employer le bon niveau de classification de sécurité

Lors de la création, de l'envoi ou du stockage d'un courriel de nature sensible, protégée ou secrète, l'utilisateur devrait s'assurer que la classification de sécurité de ce courriel n'est pas supérieure à celle du système ayant servi à le créer, l'envoyer ou le stocker.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

Un courriel ne devrait pas être créé, envoyé ou stocké dans un système ou un dépôt qui n'offre pas un niveau de sécurité équivalent (ou supérieur) au sien. Ce principe s'applique à tous les niveaux de classification de sécurité.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : lors de la création, de l'envoi ou du stockage d'un courriel de nature sensible, protégée ou secrète, l'utilisateur devrait s'assurer que la classification de sécurité de ce courriel n'est pas supérieure à celle du système utilisé pour le créer, l'envoyer ou le stocker.

5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun

Les programmes et systèmes de courriel devraient comporter des processus pour, au moment opportun, créer un compte de courriel à l'arrivée d'un employé ou d'un contractuel, le supprimer à son départ, le geler ou le suspendre pour toute raison valable.

Ces processus devraient décrire ce que les employés, les gestionnaires, les dirigeants, les administrateurs de réseaux et les spécialistes en sécurité de l'information devraient faire en diverses circonstances (et à quelle vitesse ils devraient intervenir).

« Au moment opportun » ne signifie pas nécessairement « tout de suite ». Dans le cas d'un employé qui passe d'un organisme à un autre, il est sans doute préférable de garder son compte actif tant qu'un autre compte n'a pas été ouvert chez son nouvel employeur. Dans de telles circonstances, il serait avisé de consulter un spécialiste en sécurité de l'information quant à la meilleure façon de procéder.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

Dans certains cas, un employé ou un contractuel qui entre en fonction dans une institution pourrait ne pas être en mesure d'effectuer de manière productive le travail pour lequel il a été engagé, s'il n'a pas accès rapidement à un compte de courriel chez son nouvel employeur.

Lorsqu'un employé ou un contractuel commence ou quitte un emploi, cette personne, ainsi que son gestionnaire, les dirigeants de l'organisme et les administrateurs de réseaux, ont tous une part de responsabilité par rapport au courriel.

Dès son arrivée, le nouvel employé devrait ouvrir une session, créer un mot de passe, et se familiariser avec le système de courriel. Il devrait aussi s'informer de son rôle par rapport à la gestion des courriels et de l'information associée.

Les employés devraient être avisés qu'avant de quitter leur poste pour une autre organisation, il leur faudra nettoyer leur compte de courriel, c'est-à-dire supprimer les messages éphémères, conserver et classer tous les messages qui peuvent présenter un intérêt à long terme. Dans le cas d'une absence temporaire, les employés devraient être informés qu'ils devront déléguer à une autre personne l'accès à leur courriel. À l'occasion d'une mutation interne, les employés qui souhaitent prendre avec eux certaines informations doivent d'abord en obtenir l'autorisation.

Les gestionnaires sont responsables de veiller à ce que les nouveaux employés soient bien formés à l'utilisation du système de courriel. Ils doivent également s'assurer que les employés et les contractuels détruisent ou classent adéquatement leurs messages avant de quitter l'organisation, que l'information demeure au sein d'un groupe de personnes autorisées, que les délais de conservation soient respectés et que le travail soit délégué.

Lorsqu'il s'agit d'un congédiement, d'autres facteurs entrent en ligne de compte; il peut alors être nécessaire de conserver tous les courriels de l'employé congédié, incluant ses courriels personnels, au cas où ces informations seraient requises par l'organisme ou par l'ex-employé dans le cadre d'un appel ou d'une action en justice. Certains recommandent même que le compte d'une telle personne soit carrément gelé et conservé intact pour une période prédéterminée, correspondant aux délais normaux des procédures d'appel en cas de congédiement.

Les dirigeants de l'organisme devraient préparer des procédures pour le tri et la fermeture des comptes de courriel des employés dans diverses circonstances.

Les administrateurs de réseaux ont la responsabilité de créer et de fermer les comptes de courriel des employés, ou à tout le moins de mettre fin à l'accès d'un employé à son compte, après son départ.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les programmes et systèmes de courriel en place doivent comporter des procédures permettant de réagir promptement à l'arrivée, au départ ou à la réaffectation d'un employé, d'un contractuel ou d'un autre type d'utilisateur.

Ces procédures doivent décrire ce que les employés, les gestionnaires, les dirigeants et les administrateurs de réseaux devraient faire en diverses circonstances (et à quelle vitesse).

- Lors de l'arrivée d'un nouvel employé ou d'un nouveau contractuel dans l'organisme
- Lors d'une absence temporaire d'un employé (congé, maladie, maternité, etc.)
- Lors de la démission d'un employé ou à la fin du mandat d'un contractuel
- Lors du transfert d'un employé dans une autre direction ou institution
- Lors du congédiement d'un employé ou à la fin de sa période d'emploi

Ces procédures doivent tenir compte de l'applicabilité ou non de diverses étapes.

- Déléguer l'accès au compte de courriel, et déterminer le type d'accès à déléguer
- Supprimer les messages qui ne sont pas reliés aux activités de l'organisation, ainsi que les messages éphémères
- Classifier et classer les courriels à garder, et leur fixer un délai de conservation
- Identifier les messages qui demandent un suivi, et les transmettre à un autre employé à cette fin
- Décider si certaines informations de ce compte devraient être partagées, et avec qui
- Garder le compte ouvert tout en mettant un terme à l'accès de l'ancien employé, ou le fermer complètement

Lors d'un congédiement, d'autres facteurs doivent être pris en considération.

- Décider s'il est nécessaire de conserver tous les courriels de la personne congédiée, incluant ses courriels personnels, au cas où ces informations seraient requises :
 - par l'organisme, s'il faut entreprendre une action en justice contre cet ex-employé
 - par l'ex-employé, qui a le droit d'utiliser ses anciens documents pour se défendre
- Décider si l'ensemble du fichier doit être gelé, dans le cas où l'employé a droit à une période d'appel

5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel

L'accès aux informations et aux documents contenus dans les comptes et les dossiers de courriel devrait être limité à ceux qui en ont besoin pour leur travail.

La plupart des personnes ayant un accès autorisé à leur boîte aux lettres individuelle devraient pouvoir créer, modifier et supprimer des messages, ainsi que les classer dans des dossiers.



La capacité de lire, de marquer, « d'envoyer au nom de », ou d'ajouter des messages à des dossiers peut être déléguée à un ou plusieurs collègues de travail au sein de la même unité. Des règles devraient être mises en place pour encadrer de telles délégations.

Certaines personnes autorisées peuvent recevoir une autorisation de « lecture seulement ». Afin de limiter les risques de perdre des informations importantes, seul un nombre restreint de personnes devrait avoir la possibilité de supprimer des messages dans un dossier.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Le principe de base est que les administrateurs de réseaux devraient permettre l'accès à l'information uniquement à ceux qui en ont besoin pour leur travail.

La capacité de lire, de marquer, « d'envoyer au nom de », ou d'ajouter des messages à des dossiers peut être très utile dans un groupe de travail. Or, une personne peut déléguer cette capacité à un ou plusieurs collègues à l'intérieur de son unité de travail.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'accès aux informations et aux documents contenus dans les comptes et les dossiers de courriel doit être limité à ceux qui en ont besoin pour leur travail.

La plupart des personnes ayant un accès autorisé à leur boîte aux lettres individuelle devraient pouvoir créer, modifier et supprimer des messages, ainsi que les classer dans des dossiers.

La capacité de lire, de marquer, « d'envoyer au nom de », ou d'ajouter des messages à des dossiers peut être déléguée à un ou plusieurs collègues de travail à l'intérieur de la même unité. Cependant, afin de limiter les risques de perdre des informations importantes, seul un nombre restreint de personnes devrait avoir la possibilité de supprimer des messages dans un dossier.



5.11. Utiliser des mesures de protection et d'authentification des messages

Les programmes et systèmes de gestion des courriels devraient offrir des mesures de protection et d'authentification des messages afin d'empêcher les utilisateurs ou les administrateurs de modifier un message une fois qu'il a été envoyé à au moins un destinataire, ceci afin de faciliter l'authentification et le contrôle des versions.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

L'authenticité d'un document est une mesure de la confiance que l'on peut avoir qu'un courriel est bien le document original et vrai – ou, dans le cas des supports électroniques, qu'il s'agit d'une copie conforme du message d'origine. Dans ce contexte, l'intégrité est définie comme le fait, pour un document, d'avoir été préservé sans subir aucune altération. Voilà deux importants concepts juridiques en matière de preuve.

Les mesures de protection et d'authentification empêchent un utilisateur ou un administrateur de modifier un message une fois qu'il a été envoyé à au moins un destinataire. Quand ces mesures sont en place, un message ne peut être modifié à moins d'être expédié en tant que nouveau message, avec de nouvelles données de transmission et de réception. Les mesures de protection des messages contribuent à assurer l'authenticité, l'intégrité, la fiabilité et le contrôle des différentes versions des courriels.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : des mesures de protection des messages devraient être mises en place afin de contribuer à assurer l'authenticité, l'intégrité, la fiabilité et le contrôle des différentes versions des courriels.

Ces mesures devraient empêcher les utilisateurs ou les administrateurs de modifier un message une fois qu'il a été envoyé à au moins un destinataire. Quand ces mesures sont en place, un message ne peut être modifié à moins d'être envoyé en tant que nouveau message, avec de nouvelles données de transmission et de réception.



5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre

Les programmes et systèmes de courriel devraient effectuer régulièrement des copies de sécurité, de manière uniforme, afin de répondre aux besoins opérationnels de l'organisme.

- Les copies de sécurité devraient être vérifiées afin de s'assurer qu'elles ont été faites correctement.
- Les copies de sécurité devraient être gardées dans un autre édifice.
- Les copies de sécurité devraient être recyclées régulièrement, conformément au calendrier de conservation de l'institution.
- Les procédures de copie devraient être documentées et gérées de façon à prouver qu'elles répondent aux normes.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les copies de sécurité offrent une mesure de protection en cas de perte de documents lors d'un sinistre, tels un feu, une inondation ou un tremblement de terre. Les copies de sécurité doivent toujours être conservées dans un autre édifice, de façon à réduire le risque que les originaux et les copies soient perdus en même temps, ce qui pourrait arriver si les deux étaient conservés au même endroit.

Veuillez prendre note que, normalement, les copies de sécurité sont recyclées régulièrement et ne sont pas conçues pour distinguer les sujets ou les délais de conservation. Les copies de sécurité constituent une mesure de réduction des risques, et non pas un mode de gestion de l'information.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.



(Nom de l'institution) adopte la politique suivante : les courriels et l'information associée doivent faire l'objet d'une copie de sécurité selon le calendrier suivant.

Des copies de sécurité seront effectuées (tous les jours, une fois par semaine, autre) et seront transférées dans un autre édifice où elles seront conservées pendant trois (jours, semaines, mois, années), après quoi les bandes (ou autre support de sauvegarde) pourront être recyclées.

5.13. Utiliser la signature numérique s'il y a lieu

La signature numérique devrait être utilisée dans une correspondance ou une transaction, lorsque le destinataire a besoin de savoir, hors de tout doute, que le message provient d'un expéditeur fiable, que le message n'a pas été modifié et que l'expéditeur ne pourra jamais nier qu'il l'a envoyé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaire des opérations	Dirigeants

Justification

En pratique, une signature numérique est tout simplement un nombre. Une formule est utilisée pour déterminer une valeur numérique à partir d'un message signé et pour combiner celle-ci à un nombre secret associé à l'expéditeur.

Une signature numérique est virtuellement impossible à contrefaire et elle constitue un des meilleurs moyens d'authentifier un courriel. Elle peut être vérifiée automatiquement, et cette technologie pourra aussi détecter la moindre tentative de modification du message original. La signature numérique s'appuie sur une technologie appelée chiffrement à clé publique, ou infrastructure à clé publique (ICP).

Pour avoir une signature numérique, il faut d'abord obtenir d'un gestionnaire autorisé, la permission de demander un certificat numérique. Le certificat numérique contient le nom de la personne, un numéro de série, une date d'expiration et la signature numérique de la personne, ainsi que la signature numérique de l'autorité de certification. Le certificat sert à confirmer les l'identité d'une personne lorsqu'elle mène des affaires ou des transactions. Un ministère peut émettre ses propres certificats ou les obtenir d'un fournisseur commercial fiable.

Bibliothèque et Archives Canada déclare :

Une signature numérique attribue trois qualités à un document électronique : l'intégrité, l'authentification et la non-répudiation des données. Une vérification réussie de la signature numérique permet au



Bibliothèque et Archives Canada déclare :

récepteur de s'assurer que le « document reçu » est identique au « document expédié » (intégrité des données) et de confirmer l'identité de l'expéditeur (authentification). Elle empêche également l'expéditeur de répudier le document (non-répudiation). Ces preuves sont d'une extrême importance à la réception du document, mais cette importance diminue lorsque le récepteur décide de s'en servir.

Source : Lignes directrices concernant les documents chiffrés et signés numériquement selon une infrastructure à clé publique –

<http://www.collectionscanada.gc.ca/gestion-information/002/007002-3015-f.html>

Note : Même si une signature numérique authentifie un courriel et empêche qu'il soit modifié, elle ne cache pas le contenu du message; elle ne devrait pas être confondue avec le chiffrement (qui sert à empêcher les personnes non autorisées de lire le message).

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : la signature numérique devrait être utilisée, dans une correspondance ou une transaction, lorsque le destinataire a besoin de savoir, hors de tout doute, que le message provient d'un expéditeur fiable, que le message n'a pas été modifié, et que l'expéditeur ne pourra jamais nier qu'il l'a envoyé.

Une signature numérique n'est accordée que grâce à l'émission d'un certificat numérique par une autorité de certification approuvée et fiable. Le certificat numérique contient le nom de la personne, un numéro de série, une date d'expiration et la signature numérique de la personne, ainsi que la signature numérique de l'autorité de certification. Le certificat sert à confirmer l'identité d'une personne lorsqu'elle mène des affaires ou des transactions. Un ministère peut émettre ses propres certificats ou les obtenir d'un fournisseur commercial fiable.

Choisir l'une des options suivantes :

Option 1. (Nom de l'institution) gère une infrastructure à clé publique (ICP), qui fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et offerte selon les besoins, les menaces ou les risques éventuels. Pour avoir une signature numérique, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet de l'institution à l'adresse suivante (adresse web).

Option 2. (Nom de l'institution) s'abonne à une infrastructure à clé publique (ICP) gérée par Travaux publics et Services gouvernementaux Canada (TPSGC). L'ICP fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et offerte selon les besoins, les menaces ou les risques éventuels. Pour avoir une signature numérique, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet de l'institution à l'adresse suivante (adresse web).



Option 3. L'organisme s'abonne à une infrastructure à clé publique (ICP) gérée par (un fournisseur commercial fiable). L'ICP fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et offerte selon les besoins, les menaces ou les risques éventuels. Pour avoir une signature numérique, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet de l'institution à l'adresse suivante (adresse web).

5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada

Normalement, une signature numérique n'empêche pas d'avoir accès au contenu, au contexte ou à la structure d'un courriel. Les signatures numériques qui empêcheraient cet accès devraient être enlevées des messages destinés à être transférés à Bibliothèque et Archives Canada.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Une signature numérique perd de son importance une fois que le destinataire a reçu le courriel et pris une décision ou effectué un suivi quelconque en réponse à l'information qu'il contient.

Bibliothèque et Archives Canada déclare :

Bibliothèque et Archives Canada, pour sa part, continue de confirmer l'intégrité et l'authentification de tout document d'après son emplacement dans le système de gestion des documents d'une organisation au cours des activités habituelles de celle-ci et selon la preuve que cette organisation se fait sur les documents de ce système.

Bibliothèque et Archives Canada n'essaye pas de conserver l'habileté de revérifier la signature numérique après le transfert des documents ou de conserver les traces d'une signature numérique produite d'après le système actuel d'ICP du gouvernement du Canada. De plus, Bibliothèque et Archives Canada refuse tout document rendu illisible par la présence d'une signature numérique, mais acceptera tout document dont le contenu, le contexte et la structure, exception faite de la signature numérique, sont restés intelligibles et dont l'authenticité peut être confirmée d'après son emplacement dans le système de gestion des documents d'une organisation. Il est important de noter que l'incapacité de déchiffrer les



Bibliothèque et Archives Canada déclare :

documents préalablement chiffrés peut constituer l'élimination de fait des documents conformément à l'article 12(1) de la Loi sur la Bibliothèque et les Archives du Canada.

Source : Lignes directrices concernant les documents chiffrés et signés numériquement selon une Infrastructure à clé publique –

<http://www.collectionscanada.gc.ca/gestion-information/002/007002-3015-f.html>

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante, conformément aux directives de Bibliothèque et Archives Canada : les signatures numériques seront enlevées des documents à archiver. La capacité de lire un courriel accompagné d'une signature numérique et la capacité d'enlever cette signature numérique doivent être maintenues tant que la signature numérique n'aura pas effectivement été enlevée, à un moment prévu durant la période de conservation du courriel ou à l'expiration de son délai de conservation, avant qu'il ne soit versé à Bibliothèque et Archives Canada.

5.15. Ne pas employer de signature numérisée pour signer un courriel

Les utilisateurs ne devraient jamais employer de signature numérisée pour signer un courriel, car une telle signature n'authentifie aucunement le courriel. De plus, le risque existe que cette signature soit copiée et intégrée à des documents falsifiés.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

Les utilisateurs sont mis en garde de ne jamais employer de signature numérisée, en aucune circonstance. Une telle signature n'est qu'une pièce jointe numérisée – ce n'est pas une signature numérique.



Une signature manuelle peut facilement être reproduite sous forme d'image à l'aide d'un numériseur, mais il est dangereux d'utiliser cette image en guise de signature d'un message ou d'une pièce jointe, afin de simuler la véritable signature de son expéditeur.

Le danger est le suivant : une personne malhonnête peut tout aussi aisément copier-coller cette image de signature dans un autre document électronique et ainsi fabriquer un faux. Une telle contrefaçon est si facile à faire qu'une signature numérisée a peu de chance d'être acceptée en preuve par un tribunal ou lors d'un audit.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : il est interdit d'utiliser, dans un document électronique, l'image d'une signature numérisée à la place d'une signature manuelle, pour quelque type de correspondance que ce soit, y compris le courriel.

5.16. Utiliser le chiffrement s'il y a lieu

Le chiffrement peut être utilisé, s'il y a lieu, pour accroître la sécurité d'un courriel et de ses pièces jointes durant la période de stockage ou lors d'une transmission.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Le chiffrement consiste à remplacer le texte d'un message ou de pièces jointes par un code que seuls les destinataires autorisés sont capables de déchiffrer afin de reconstituer le texte original. Les enfants connaissent bien le code, très simple, qui consiste à remplacer les lettres de l'alphabet par un chiffre (A = 1, B = 2, C = 3, etc.). Les technologies modernes de chiffrement utilisent des codes infiniment plus complexes, mais elles peuvent chiffrer un message (c'est-à-dire appliquer le code) et le déchiffrer d'une simple pression d'un bouton



L'utilisation du courriel n'est pas recommandée pour la transmission de messages et de pièces jointes qui contiennent de l'information sensible, protégée ou secrète. Cependant, dans certaines circonstances définies par la politique de sécurité et autorisées par la direction de l'institution, de telles informations peuvent être transmises, du moment qu'elles sont chiffrées au moyen d'un système de chiffrement approuvé par le gouvernement du Canada.

Habituellement, les logiciels de sécurité offrent à la fois la capacité de chiffrer l'information et celle d'ajouter une signature numérique. Pour avoir une signature numérique et la capacité de chiffrer des courriels et d'autres documents, il faut d'abord obtenir d'un gestionnaire autorisé la permission de demander un certificat numérique. Une signature numérique n'est accordée que grâce à l'émission d'un certificat numérique par une autorité de certification approuvée et fiable. Le certificat numérique contient le nom de la personne, un numéro de série, une date d'expiration et la signature numérique de la personne, ainsi que la signature numérique de l'autorité de certification. Le certificat sert à confirmer l'identité d'une personne lorsqu'elle mène des affaires ou des transactions. Un ministère peut émettre ses propres certificats ou les obtenir d'un fournisseur commercial fiable.

Voir : Politique de gestion de l'Infrastructure à clé publique au gouvernement du Canada
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_f.asp

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : le chiffrement devrait être utilisé, dans une correspondance ou une transaction, lorsque l'expéditeur a besoin d'être assuré, hors de tout doute, que seul le destinataire prévu pourra lire son message, et que celui-ci sera illisible pour toute autre personne, quel qu'en soit le format électronique.

Une technologie de chiffrement n'est accordée que grâce à l'émission d'un certificat numérique par une autorité de certification approuvée et fiable. Le certificat numérique contient le nom de la personne, un numéro de série, une date d'expiration et la signature numérique de la personne, ainsi que la signature numérique de l'autorité de certification. Le certificat sert à confirmer l'identité d'une personne lorsqu'elle mène des affaires ou des transactions et permet à son utilisateur de chiffrer des messages de telle manière qu'ils ne puissent être déchiffrés et lus, sous forme électronique, que par le destinataire prévu. Un ministère peut émettre ses propres certificats ou les obtenir d'un fournisseur commercial fiable.

Choisir l'une des options suivantes :

Option 1. (Nom de l'institution) gère lui-même une infrastructure à clé publique (ICP), qui fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et disponible selon les besoins, les menaces ou les risques éventuels. Pour obtenir une signature numérique et une technologie de chiffrement, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une



analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet l'institution à l'adresse suivante (adresse Web).

Option 2. (Nom de l'institution) s'abonne à une infrastructure à clé publique (ICP) gérée par Travaux publics et Services gouvernementaux Canada (TPSGC). L'ICP fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et disponible selon les besoins, les menaces ou les risques éventuels. Pour obtenir une signature numérique et une technologie de chiffrement, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet l'institution à l'adresse suivante (adresse Web).

Option 3. L'organisme s'abonne à une infrastructure à clé publique (ICP) gérée par (un fournisseur commercial fiable). L'ICP fournit des dispositifs de sécurité tels que la signature numérique et le chiffrement. Cette technologie est dispendieuse et disponible selon les besoins, les menaces ou les risques éventuels. Pour obtenir une signature numérique et une technologie de chiffrement, il faut d'abord obtenir un certificat numérique, émis par l'autorité de certification de l'institution. Toute demande doit être remplie et signée par le (gestionnaire, directeur, directeur général) de l'utilisateur. Il (sera ou pourra être) nécessaire d'effectuer d'abord une analyse des risques et des menaces. Toutes les instructions sont précisées sur le site Intranet l'institution à l'adresse suivante (adresse Web).

5.17. Employer le stockage de proximité pour la conservation à long terme des courriels

Les courriels, ainsi que leurs métadonnées et pièces jointes, qui doivent être conservés pendant un certain temps devraient être stockés dans un système électronique de gestion de l'information, distinct du système de courriel.

Les courriels, leurs métadonnées et pièces jointes devraient être conservés ensemble; ou, si ces éléments sont stockés séparément, il devrait être possible de reconstituer la relation qui les unit, de sorte que l'authenticité et l'intégrité de ces éléments, et leur relation, puissent être démontrées en cour.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les systèmes de courriel ne sont pas conçus pour la conservation à long terme des messages et de leurs pièces jointes. Leur performance décroît à mesure que la quantité de mémoire requise pour le stockage dépasse un certain seuil.

Il est plus efficace de conserver les courriels à long terme dans des systèmes autres que le système de courriel.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

Option 1. (Nom de l'institution) adopte la politique suivante : une seule copie des courriels, de leurs métadonnées et pièces jointes sera stockée dans une base de données à l'échelle du gouvernement canadien.

Les courriels, leurs métadonnées et pièces jointes sont reçus ou créés à l'aide des logiciels de l'institution (Lotus, Ms Outlook, ou autre). Les courriels, métadonnées et pièces jointes sont automatiquement transférés dans un dépôt central (géré par le gouvernement du Canada et partagé par plusieurs organismes). Une fois les documents transférés, l'expéditeur et tous les destinataires prévus y ont accès, comme s'ils étaient stockés en ligne.

Option 2. (Nom de l'institution) adopte la politique suivante : une seule copie des courriels, de leurs métadonnées et pièces jointes sera stockée dans une base de données à l'échelle du gouvernement canadien.

Les courriels, leurs métadonnées et pièces jointes sont reçus ou créés à l'aide des logiciels de l'institution (Lotus, Ms Outlook, ou autre). Les courriels, métadonnées et pièces jointes sont automatiquement transférés dans un dépôt central (géré par l'institution). Une fois les documents transférés, l'expéditeur et tous les destinataires prévus y ont accès, comme s'ils étaient stockés en ligne.

Option 3. (Nom de l'institution) adopte la politique suivante : les courriels seront stockés dans un système conventionnel où les courriels eux-mêmes, leurs métadonnées et pièces jointes peuvent être reproduits plusieurs fois.

Les messages créés ou reçus par les utilisateurs de (nom de l'institution) peuvent être stockés en ligne, mais pour une durée limitée seulement. Les utilisateurs peuvent garder en ligne, tant qu'ils sont utiles, des documents éphémères ou qui ne sont pas considérés comme des documents organisationnels; ils pourront ensuite les détruire. Cependant, les utilisateurs doivent réviser leurs messages au moins une fois par semaine, afin de décider quels messages garder et quels messages détruire. Les courriels qui sont considérés comme étant de l'information ou des documents organisationnels devraient être classés dans un système approuvé de stockage de proximité.

5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore

Au gouvernement du Canada, on ne privilégie pas la conservation de copies papier de documents électroniques. Toutefois, la conservation de courriels sur support papier peut être appropriée dans le cas de petits organismes disposant de ressources technologiques limitées. Cette méthode peut aussi convenir pour les documents à haut risque.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Il y a des avantages et des inconvénients à imprimer des courriels et à les conserver sur support papier.

Le principal avantage est que, si l'impression est faite sur du papier sans acide de qualité archives, et que le document est conservé dans des conditions optimales, ce document et l'information qu'il contient se conserveront pendant des millénaires, alors que la durée de vie de la plupart des supports magnétiques se mesure en années, ou au mieux en décennies. Les supports optiques sont sensiblement plus durables que les supports magnétiques, mais rien ne prouve encore qu'ils pourront se conserver aussi longtemps que le papier.

Il y a cependant plusieurs inconvénients majeurs à l'impression sur papier.

- Les organismes savent que les coûts reliés à l'indexation, à la recherche et à la récupération de copies papier sont beaucoup plus élevés que ceux reliés au stockage et à la gestion de copies électroniques.
- Les métadonnées sont souvent considérées comme importantes lors d'actions en justice; il faut donc les imprimer aussi et les ranger avec les messages auxquels elles sont associées, ce qui ajoute une étape supplémentaire au processus d'entreposage.
- Le papier n'est pas très performant quand il s'agit de conserver des pièces jointes telles que des feuilles de calcul, des petites bases de données, des fichiers audio, vidéo ou multimédia, des dessins en 3D, des rendus d'architecture en 3D, des cartes en teintes hypsométriques, etc. tous des produits typiques de l'âge électronique.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : la méthode à privilégier pour conserver de l'information et des documents électroniques est le stockage électronique.

Un document qui a d'abord été produit sur papier peut être classé et conservé sous cette forme, conformément aux procédures établies par le gestionnaire de l'information de (nom de l'institution).

Un document qui a d'abord été produit sur papier peut aussi être numérisé et reproduit en format électronique, puis rangé dans un système de stockage électronique. Le document d'origine sera ensuite éliminé conformément aux procédures établies par le gestionnaire de l'information de (nom de l'institution).



Si un document électronique est imprimé à des fins de classement et d'entreposage, ses métadonnées devraient aussi être imprimées et jointes au document sur support papier. Le document électronique sera ensuite éliminé conformément aux procédures établies par le gestionnaire de l'information de (nom de l'institution).

5.19. Protéger les courriels en protégeant les supports de conservation

Un programme de gestion des courriels devrait être capable de protéger les supports de conservation au même titre que les informations électroniques, et devrait régulièrement vérifier les données stockées afin de détecter d'éventuelles pertes d'informations.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les supports de conservation électroniques sont extrêmement fragiles, vulnérables aux champs magnétiques et aux dommages physiques. Même s'ils sont bien protégés, les supports tels que les CD-ROM, les DVD ou les bandes magnétiques se dégradent rapidement (d'un point de vue archivistique) – parfois en moins de dix ans. De plus, la conservation d'informations électroniques présume que les logiciels et les équipements requis pour lire les informations en question seront encore disponibles dans les années à venir.

Les supports magnétiques, tels les rubans, les disquettes et les disques rigides, peuvent durer de 10 à 20 ans s'ils sont conservés avec soin; cependant, ils sont très vulnérables à certaines conditions physiques comme l'abrasion, ou la sécheresse, l'humidité, la chaleur et le froid excessifs. Ils craignent aussi les moisissures et les acariens, et sont, bien entendu, très vulnérables aux variations des champs magnétiques.

Les supports optiques, tels que les CD, sont un peu plus durables et peuvent probablement se conserver une centaine d'années, à condition d'être traités et entreposés avec grand soin.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter



L'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les courriels et l'information associée, conservés sur des supports magnétiques, (seront / devraient être) protégés de toute menace telle que : saleté, poussière, acariens, moisissures, oxydation, réactions chimiques, températures ou humidité extrêmes.

À des intervalles appropriés, on devrait faire migrer l'information électronique vers des équipements et des logiciels plus récents, afin de s'assurer qu'elle demeure lisible. Notez bien que les logiciels et les équipements actuels seront probablement oubliés dans 15 ans.

Il faudrait aussi effectuer régulièrement des vérifications, par échantillonnage, des données conservées afin d'évaluer le degré de perte d'information; un seuil maximum devrait être établi, au-delà duquel il faudra procéder à la migration.

5.20. Protéger les courriels de l'obsolescence

Un programme de gestion des courriels devrait protéger ceux-ci contre l'obsolescence des logiciels et des équipements requis pour lire les messages et leurs pièces jointes.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------

Justification

Les équipements et les supports de stockage électroniques évoluent très rapidement. Même si on parvenait à conserver intégralement les courriels, leurs métadonnées et pièces jointes, il y aurait encore un risque que les équipements et les logiciels requis pour les lire ne soient plus disponibles dans 20 ans – ou alors que personne dans l'organisation ne se souvienne comment ils fonctionnent.

Voici trois solutions possibles à ce problème.

- Conserver les logiciels qui peuvent actuellement lire les fichiers, ainsi que des équipements en nombre suffisant pour simuler l'environnement dans lequel les courriels ont été créés ou reçus. Cette approche conviendra pendant un certain temps, mais pas à très long terme.
- Procéder immédiatement à la migration des fichiers dans un format standard qui n'est pas dépendant de logiciels ou d'équipements en particulier. Ceci présente l'avantage de rendre l'information « universellement » lisible. Cependant, une grande partie du formatage et du



contexte d'origine sera perdue. Cette approche ajoute aussi une étape supplémentaire au processus.

- Faire migrer les fichiers vers des versions plus récentes du système dans lequel ils ont été créés. Ceci présente l'avantage que les nouvelles versions de logiciels permettent normalement de lire et de reproduire fidèlement des documents créés ou reçus à l'aide de versions antérieures. De fréquentes migrations risquent toutefois de créer des distorsions dans les courriels; les procédures de migration devraient être testées afin de prévenir de telles distorsions.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les courriels et l'information associée seront protégés et des mesures seront prises afin qu'ils demeurent lisibles, en format électronique, pendant toute la durée de conservation appropriée.

5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel

La documentation relative à un système de gestion des courriels devrait pouvoir, au moment opportun, fournir des preuves raisonnables de la condition du système, ainsi que de l'authenticité et de l'intégrité des courriels, de leurs métadonnées et pièces jointes, au cours de la période pertinente, dans le contexte de l'action juridique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Afin de prouver en cour l'authenticité, l'intégrité et la fiabilité des courriels, de leurs métadonnées et pièces jointes, il pourrait s'avérer nécessaire de prouver aussi la fiabilité et l'intégrité du système qui a servi à les créer, les expédier, les recevoir et les stocker. La documentation de système devra être complète, précise, à jour, et couvrir la période de temps appropriée.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : une documentation complète des programmes et des systèmes de courriels sera constituée, tenue à jour et conservée. Cette documentation devra permettre de confirmer, avec un degré raisonnable de certitude, que les courriels fournis en preuve à l'occasion d'une action en justice ou d'un audit, sont (ou ne sont pas) des preuves fiables. Au minimum, la documentation doit pouvoir établir les faits suivants :

- Le système fonctionnait normalement au moment de la création, de la réception, du stockage et de la récupération du courriel.
- Le système a continué de fonctionner normalement après la création, la réception, le stockage et la récupération du courriel.
- Si le système n'a pas fonctionné normalement à un moment donné, les courriels n'ont pas été affectés.
- Le système lui-même n'a pas été modifié après la création ou la réception du courriel.
- Si le système a été modifié à un moment donné, les courriels pertinents n'ont pas été affectés.
- Si le système a modifié le courriel, ses métadonnées et pièces jointes, les modifications ont été négligeables.
- Les normes et directives du gouvernement canadien en matière de sécurité des systèmes ont été appliquées correctement et systématiquement.
- Le système a fait l'objet de copies de sécurité régulières et systématiques.
- Les données et les pistes de vérification sont régulièrement enregistrées afin de prouver la fiabilité des courriels.
- La copie officielle des messages a été dûment identifiée et conservée adéquatement.
- Les procédures de copie de sécurité ont été coordonnées avec la disposition des courriels.
- Aucune copie d'un document n'est conservée après l'expiration de son délai de conservation.

5.22. Conserver en permanence la documentation du système de courriel

La documentation de système devrait être considérée comme un document gouvernemental à conservation permanente, et devrait donc être traitée et entreposée en conséquence.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

Afin de prouver en cour l'authenticité, l'intégrité et la fiabilité des courriels, de leurs métadonnées et pièces jointes, il pourrait s'avérer nécessaire de prouver aussi la fiabilité et l'intégrité du système grâce auquel ils ont été créés, reçus ou stockés.

Un document n'est généralement pas admissible en preuve s'il n'est pas jugé fiable par la cour. Une partie qui ne peut produire suffisamment de preuves fiables risque de ne pas pouvoir plaider sa cause adéquatement. Pire, une partie incapable de produire suffisamment de preuves fiables peut être considérée comme faisant défaut, et la cour tranchera alors en faveur de l'autre partie.

Comme il est impossible de savoir ou de prédire à quel moment il sera nécessaire d'établir une preuve en cour, la documentation de système doit être conservée en permanence.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : une documentation complète des systèmes et des programmes de courriel sera constituée et tenue à jour; elle sera conservée (ainsi qu'une copie de sécurité dans un autre endroit) à titre de document d'archives permanent.

5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes

Le système de gestion des courriels doit être configuré de façon à pouvoir gérer à la fois un message dont le délai de conservation vient tout juste de commencer, et une pièce jointe dont le délai est sur le point d'expirer, que les messages et leurs pièces jointes soient conservés ensemble ou séparément. Il convient de rappeler que les délais de conservation sont établis en fonction du contenu de l'information et non en fonction du système qui a servi à créer, transmettre ou stocker cette information. Cela constitue un problème difficile et pose de réels défis techniques. Il est fortement recommandé de consulter un conseiller juridique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

Les documents gouvernementaux ont des délais de conservation qui varient en fonction de leur contenu ou de leur classification. Certains documents doivent être conservés pendant une durée minimale, laquelle peut varier. D'autres, notamment ceux qui contiennent des renseignements personnels, ont un délai de conservation maximal et doivent être éliminés à l'expiration de ce délai.

Dans les deux cas, le délai de conservation peut être prolongé si les documents sont requis en preuve lors d'une action en justice ou d'un audit.

Il est très possible qu'un courriel, dont le délai de conservation commence à peine, contienne une pièce jointe dont le délai de conservation est à la veille d'expirer. Le système de gestion des courriels doit être capable de gérer adéquatement ces différences entre les délais.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : le système de gestion des courriels utilisé par (nom de l'institution) (doit / devrait être) être capable de gérer adéquatement des délais de conservation différents pour un courriel et ses pièces jointes, par exemple, dans le cas où un courriel commence son délai de conservation alors qu'une de ses pièces jointes achève le sien.

Lorsque le délai de conservation d'un courriel expire quelque temps après le délai minimal de conservation d'une pièce jointe, la date d'élimination de la pièce jointe doit être reportée pour rejoindre celle du courriel.

Lorsque le délai de conservation d'un courriel expire quelque temps après le délai maximal de conservation d'une pièce jointe, la pièce jointe doit être éliminée au moment prévu. Le courriel sera conservé pour la balance de son propre délai de conservation.

Prenez note qu'il faut aussi pouvoir appliquer un ordre de retenue sur tout document (courriel, métadonnées ou pièces jointes) pour en empêcher la destruction, que celle-ci ait été prévue ou non au calendrier, et qu'elle soit volontaire ou non, si ledit document doit être produit en preuve dans le cadre d'un audit ou d'une action en justice.

5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document

Les systèmes et programmes de gestion des courriels devraient avoir la capacité de repérer les courriels et l'information associée destinés à être éliminés afin, au besoin, de les isoler et de les protéger contre une destruction, qu'elle soit bien ou mal intentionnée, ou accidentelle.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Certaines informations et certains documents gouvernementaux sont assujettis par la loi à des délais de conservation maximaux et doivent être éliminés à l'expiration de ces délais. Conserver de telles informations au-delà du délai prescrit constitue une infraction, à moins qu'elles ne soient requises dans le cadre d'une action en justice, d'un audit ou d'une demande d'accès à l'information. Dans de telles circonstances, le délai de conservation peut être prolongé aussi longtemps que nécessaire.

Notez bien que les tribunaux ont déjà rendu des décisions défavorables à l'encontre de parties qui avaient détruit de l'information requise en preuve – même si cette destruction avait eu lieu conformément à un calendrier de conservation approuvé de longue date. De telles décisions s'appuient sur le principe que les parties savaient ou auraient dû savoir qu'une telle information allait être requise dans le cadre de certaines actions en justice, et qu'elles auraient dû appliquer un ordre de retenue pour empêcher la destruction des documents.

Plus encore, les tribunaux ont déjà rendu des jugements défavorables à l'encontre de parties qui avaient détruit de l'information, en invoquant que les parties en question auraient dû prévoir que cette information, en raison même de sa nature, pourrait un jour être exigée en preuve dans le cadre d'une éventuelle action en justice.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique qui suit.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les systèmes et programmes de gestion des courriels doivent avoir la capacité de repérer les courriels et l'information associée destinés à être détruits et, au besoin, les isoler et les protéger contre une destruction bien intentionnée, mal intentionnée ou accidentelle, grâce à l'application d'un ordre de retenue.

Certaines informations et certains documents gouvernementaux sont assujettis par la loi à des délais de conservation maximaux et doivent être éliminés à l'expiration de ces délais. Conserver de telles informations au-delà du délai prescrit constitue une infraction, à moins que ces informations ne soient requises dans le cadre d'une action en justice, d'un audit ou d'une demande d'accès à l'information. Dans de telles circonstances, le délai de conservation peut être prolongé aussi longtemps que nécessaire.



Les fichiers destinés à l'élimination doivent être évalués, avant d'être détruits, en fonction de leur pertinence par rapport à toute action en justice ou tout audit, connus, en attente, ou potentiels. S'ils sont jugés pertinents, ou susceptibles d'être pertinents pour une action en justice ou un audit, un ordre de retenue doit être appliqué.

Tout ordre de retenue devrait être réexaminé annuellement et annulé s'il y a lieu. Un tel ordre peut être annulé si les documents auxquels il s'applique ont été conservés aux fins d'une action en justice ou d'un audit, maintenant terminés, et qu'il n'est pas prévu de faire appel.

Si un employé est au courant qu'un audit ou qu'une action en justice impliquant son institution est en cours, ou qu'il a des raisons de croire qu'une telle action est imminente ou qu'elle pourrait se produire dans l'avenir, cet employé devrait informer (le conseiller juridique), qui informera à son tour (le gestionnaire de l'information) de la pertinence de tout courriel et de toute information associée, de façon à ce qu'un ordre de retenue soit imposé, au besoin.



6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes

En vertu des articles 12 (1) et 13 (1) de la Loi sur la Bibliothèque et les Archives du Canada (2004), aucun document gouvernemental ne peut être éliminé sans une autorisation écrite du bibliothécaire et archiviste du Canada. Il est important d'éliminer régulièrement les courriels éphémères et les copies de courriels (incluant les copies latentes, c'est-à-dire supprimées, mais non écrasées). Cependant, il est essentiel de pouvoir empêcher l'élimination ou la modification de documents requis (ou pouvant être requis) dans le cadre d'un audit, d'une action en justice ou d'une demande d'information en vertu de l'AIPRP.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Il sera possible de démontrer un degré élevé de conformité aux calendriers de conservation institutionnels, aux autorisations de disposer des documents, approuvées par Bibliothèque et Archives Canada, et aux autres obligations découlant de lois et de politiques, en vue d'assurer au moment opportun l'élimination des courriels qui ne sont plus utiles à l'organisation.
- L'information qui, selon l'institution, possède une valeur historique sera systématiquement transférée à Bibliothèque et Archives Canada.

6.1. Obtenir une autorisation de disposition des courriels

Le bibliothécaire et archiviste du Canada a l'autorité nécessaire pour approuver la disposition de tout courriel sous le contrôle d'une institution gouvernementale et peut déléguer cette autorité à un ou plusieurs responsables dans l'institution.

Le bibliothécaire et archiviste du Canada a le pouvoir d'accorder une autorisation de disposer des documents (ADD) à une institution. Le bibliothécaire et archiviste du Canada peut aussi accorder une autorisation pluri-institutionnelle de disposer des documents (APDD) qui permet l'élimination de documents communs à plusieurs institutions.

Les responsables peuvent à leur tour déléguer aux utilisateurs le pouvoir de prendre des décisions concernant l'élimination des courriels qu'ils créent ou reçoivent, mais cette délégation doit être faite par écrit, avec référence aux présentes Lignes directrices pour la gestion des courriels.



Une infraction aux dispositions de la Loi sur la Bibliothèque et les Archives du Canada est punissable sur déclaration de culpabilité par procédure sommaire (amende / prison).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

L'article 12 (1) de la Loi sur la Bibliothèque et les Archives du Canada se lit comme suit :

L'élimination ou l'aliénation des documents fédéraux ou ministériels, qu'il s'agisse ou non de biens excédentaires d'une institution gouvernementale, est subordonnée à l'autorisation écrite de l'administrateur général ou de la personne à qui il a délégué, par écrit, ce pouvoir.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les courriels, métadonnées et pièces jointes qui sont de l'information ou des documents officiels doivent être conservés durant une période de temps appropriée (mais pas plus longtemps). À l'expiration de leur délai de conservation, les documents ou l'information devront être éliminés conformément à l'autorisation de disposition déléguée à (nom de l'institution) et administrée par le gestionnaire de l'information.

Aucun fichier ne peut être éliminé sans l'autorisation écrite du gestionnaire de l'information.

Veuillez noter que le gestionnaire de l'information ne devrait pas, normalement, être impliqué dans les décisions relatives à l'élimination de fichiers individuels. Le gestionnaire de l'information peut autoriser d'autres personnes de l'institution, incluant des utilisateurs, à éliminer certaines catégories de documents ou d'informations, à certains moments, et à certaines conditions.

Veuillez aussi noter que le délai de conservation d'un courriel peut différer de celui d'une pièce jointe.

6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun

Les programmes et systèmes de courriel devraient pouvoir repérer les fichiers de courriels à éliminer conformément au calendrier de conservation, où qu'ils se trouvent dans l'organisation, et permettre au personnel autorisé de les détruire de telle manière qu'ils ne puissent jamais être reconstitués.



Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Supprimer un courriel ne le détruit pas. La suppression détruit uniquement le lien permettant à l'utilisateur de sélectionner et d'ouvrir le fichier. Le message lui-même n'est pas éliminé tant qu'il n'est pas écrasé par un autre fichier électronique. Cela signifie que le courriel, même une fois supprimé, peut exister encore pendant des mois sur des bandes de sauvegarde, ou comme copie latente ou fichier caché, dans le système de courriel ou dans le système de gestion de l'information électronique de l'institution.

Pour être entièrement conforme à la loi qui limite la durée de conservation de certains documents et informations, il faut éliminer toutes les copies sous le contrôle de l'institution. Par conséquent, lorsque le délai de conservation d'un courriel est expiré, toutes les copies de ce courriel, incluant les copies latentes, sur tous les supports contrôlés par l'institution doivent être repérées et éliminées de telle manière qu'il soit impossible de les reconstituer.

Il existe des moyens (outils informatiques) permettant d'éliminer ou d'écraser les fichiers de façon à les rendre irrécupérables.

Il faut se rappeler que les courriels peuvent être « découverts » tant qu'ils sont récupérables. Cela signifie qu'ils peuvent être exigés en preuve, même s'ils ont été supprimés, tant qu'il est possible de les récupérer sur n'importe quel support d'enregistrement appartenant à l'institution. Permettre à des telles copies de continuer d'exister après l'expiration de leur délai de conservation aura deux conséquences : les coûts de recherche seront plus élevés parce que les chercheurs devront examiner un plus grand nombre de documents pour trouver la preuve demandée par la cour, et la cour se retrouvera avec plus de preuves que nécessaire.

L'intention d'une telle disposition est de se conformer à la loi, non de détruire des preuves.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les programmes et systèmes de courriel appartenant à (nom de l'institution) doivent pouvoir repérer les fichiers de courriels à éliminer conformément au calendrier de conservation, où qu'ils se trouvent dans l'organisation, et permettre au personnel autorisé de les détruire de telle manière qu'ils ne puissent pas être reconstitués.



Les employés, contractuels et utilisateurs du système de courriel sont, par la présente, avertis que le fait de supprimer un courriel ne le détruit pas. La suppression détruit uniquement le lien permettant à l'utilisateur de sélectionner et d'ouvrir le fichier. Le message lui-même n'est pas détruit tant qu'il n'est pas écrasé par un autre fichier électronique. Cela signifie que le courriel, même une fois supprimé, peut exister encore pendant des mois sur des bandes de sauvegarde, ou comme copie latente ou fichier caché dans un système de courriel ou dans un système de gestion de l'information électronique.

Pour être entièrement conforme à la loi qui limite la durée de conservation de certains documents et informations, il faut éliminer toutes les copies sous le contrôle de l'institution. Par conséquent, lorsque le délai de conservation d'un courriel est expiré, toutes les copies de ce courriel, incluant les copies latentes, sur tous les supports contrôlés par l'institution doivent être repérées et éliminées de telle manière qu'il soit impossible de les reconstituer.

Le (nom de l'institution) utilise les moyens suivants (fournir une liste des outils informatiques) permettant d'éliminer ou d'écraser les fichiers de façon à les rendre irrécupérables.

Les employés, contractuels et utilisateurs du système de courriel sont, par la présente, avertis que les courriels peuvent être « découverts » tant qu'ils sont récupérables. Cela signifie qu'ils peuvent être exigés en preuve, même s'ils ont été supprimés, tant qu'il est possible de les récupérer sur n'importe quel support d'enregistrement sous le contrôle de l'institution. Les courriels doivent, par conséquent, être stockés dans des emplacements approuvés.

Permettre à des telles copies de continuer d'exister après l'expiration de leur délai de conservation aura deux conséquences : les coûts de recherche seront plus élevés parce que les chercheurs devront examiner un plus grand nombre de documents pour trouver la preuve demandée par la cour, et la cour se retrouvera avec plus de preuves que nécessaire.

6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP

Les programmes et systèmes de gestion des courriels devraient pouvoir protéger les courriels et l'information associée, soit le message lui-même, ses métadonnées et pièces jointes, de toute destruction bien ou mal intentionnée, ou accidentelle, et de toute spoliation (terme juridique signifiant dommage ou altération).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Veuillez noter que les tribunaux ont déjà rendu des décisions défavorables à l'encontre de parties qui ont détruit, altéré ou endommagé des documents exigés en preuve. Ces décisions étaient fondées sur le principe juridique « *omnia praesumuntur contra spoliatorem* », signifiant « toute



chose étant présumée à l'encontre du destructeur ou du malfaiteur ». En d'autres termes, le tribunal présume que la partie qui a endommagé la preuve a quelque chose à cacher. On peut perdre un procès sur cette seule présomption.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les programmes et systèmes de courriel appartenant à (nom de l'institution) doivent avoir la capacité de protéger les courriels et l'information associée, soit le message lui-même, ses métadonnées et pièces jointes, de toute destruction bien ou mal intentionnée, ou accidentelle, et de toute spoliation (dommage ou modification).

Les tribunaux ont déjà rendu des décisions défavorables à l'encontre de parties qui ont altéré ou endommagé des documents exigés en preuve. En d'autres termes, le tribunal présume que la partie qui a endommagé la preuve a quelque chose à cacher. On peut perdre un procès sur cette seule présomption. De plus, la destruction d'une preuve peut constituer un acte criminel.



7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin

Les systèmes de courriel évoluent très rapidement. L'ajout de nouvelles caractéristiques et de nouveaux services, et une meilleure compatibilité avec d'autres modes de communication engendrent sans cesse de nouvelles formes d'utilisation. Les institutions doivent régulièrement examiner l'efficacité de leurs politiques et pratiques en matière de courriel afin de s'assurer qu'elles atteignent les objectifs visés.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Des cadres de responsabilisation seront en place afin de garantir une gestion efficace des courriels.
- Les risques, faiblesses et autres problèmes importants en matière de gestion seront identifiés, documentés et signalés, et des correctifs seront apportés s'il y a lieu.

7.1. Évaluer l'efficacité de la gestion des courriels

C'est le spécialiste en gestion de l'information (GI) qui a la responsabilité première de procéder à une évaluation périodique détaillée de la gestion des courriels dans son institution et de formuler des recommandations en vue de son amélioration. Cependant, tous les employés de l'organisation ont une part de responsabilité dans la gestion du courriel. Par conséquent, les utilisateurs, les administrateurs de réseaux ou de systèmes, les gestionnaires des opérations et les dirigeants devraient régulièrement évaluer de quelle manière ils pourraient, en tant qu'individus, contribuer plus efficacement à la gestion des courriels. Les institutions devraient mettre à la disposition de leurs employés un endroit accessible où les leçons apprises pourraient être rassemblées et partagées.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

Le spécialiste en gestion de l'information, en raison de sa formation et de son expérience poussées, est le mieux qualifié pour évaluer la gestion des courriels dans les grandes institutions. Les plus petits organismes, où la personne chargée de l'évaluation a peut-être moins de formation et d'expérience, pourront obtenir des conseils et du soutien de BAC ou du secteur privé.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'efficacité des politiques, programmes et méthodes en matière de gestion des courriels sera évaluée sur une base régulière (indiquer la fréquence appropriée). Cette évaluation devrait porter sur les points suivants (supprimer ceux qui ne sont pas pertinents).

- Les différents types de courriels et d'informations associées en usage dans l'institution
- L'efficacité des plans de classification, des notices descriptives et des métadonnées
- L'adhésion des utilisateurs aux plans de classification
- Les plans pour la GI/TI par rapport à la gestion des courriels
- Les politiques, normes et lignes directrices en GI/TI concernant la gestion des courriels
- Les méthodologies de contrôle de conformité relatives à la gestion des courriels
- Les conseils sur les investissements en technologie de l'information reliées à la gestion des courriels
- L'analyse des vérifications de conformité aux GI/TI des exercices de découverte électronique et de disposition reliés aux courriels
- Les analyses coût/bénéfice et les analyses d'impact des pratiques actuelles en matière de gestion des courriels
- L'efficacité des stratégies de communication par rapport à la gestion des courriels
- La diffusion des outils de communication relatifs à la gestion des courriels
- L'efficacité des processus permettant d'accéder aux courriels et aux informations associées
- L'efficacité et la pertinence (ou les faiblesses) de l'infrastructure et des processus reliés au stockage et à la protection des courriels et des informations associées
- L'efficacité des processus touchant l'élimination des courriels et des informations associées, et l'application d'ordres de retenue



8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Tous les employés d'une institution fédérale, incluant les agents et contractuels engagés par cette institution, comprendront leurs rôles et responsabilités en matière de gestion des courriels.
- Ces personnes appliqueront correctement à la gestion des courriels les principes de gestion du cycle de vie de l'information.
- Ces personnes veilleront à ce que les courriels soient conservés sur un support de stockage et dans un endroit appropriés, et durant une période de temps appropriée. Elles respecteront les règles d'étiquette de l'institution en matière de courriel.

8.1. Responsabilités des utilisateurs

Afin de contribuer efficacement à la gestion des courriels, les utilisateurs devraient connaître et comprendre les lois, règlements, normes, lignes directrices, politiques et procédures touchant le courriel, et devraient utiliser et gérer leurs courriels en conséquence.

L'information destinée aux utilisateurs peut prendre la forme de documents, de matériel pédagogique, d'accompagnement individuel ou de cours formels, et peut être offerte sur différents supports, et de différentes manières, selon le choix de l'institution. C'est l'institution qui doit fournir l'information à ses employés. Si ce n'est pas le cas, ceux-ci peuvent en faire la demande.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants



Justification

En matière de gestion des courriels, ce sont les utilisateurs qui se trouvent « sur la ligne de front ». Contrairement à d'autres formes de documents électroniques, habituellement gérés de façon centralisée, les courriels doivent, par nature, être gérés selon un mode décentralisé. L'utilisateur, face à son écran d'ordinateur, est la première personne à intervenir dans la gestion de ses courriels.

Normalement, c'est le créateur d'un courriel qui doit le conserver, mais dans certaines circonstances, c'est le destinataire qui est responsable de cette conservation. Les utilisateurs doivent savoir quels messages peuvent être éliminés et lesquels doivent être conservés, ainsi que l'endroit où ils doivent être stockés, et pour combien de temps.

Les utilisateurs doivent apprendre et respecter les règles d'étiquette du réseau (nétiquette), et adopter un langage et un ton appropriés lorsqu'ils rédigent leurs messages. Ils doivent également savoir quand utiliser le courriel et quand ne pas l'utiliser. Par exemple, les utilisateurs ne devraient pas communiquer des informations sensibles par courriel, mais, s'il le faut, ils devraient chiffrer leurs messages pour protéger ces informations.

Bref, les utilisateurs du courriel sont largement responsables de la gestion des courriels à tous les stades de vie de l'information. Pour s'acquitter efficacement de ces responsabilités et gérer les courriels reçus ou expédiés de manière appropriée, les utilisateurs doivent connaître et comprendre les lois, règlements, normes, lignes directrices, politiques et procédures concernant le courriel.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : (nom de l'institution) aidera les utilisateurs du courriel à comprendre les lois, règlements, normes, lignes directrices, politiques et procédures concernant le courriel, et à utiliser et gérer leurs courriels en conséquence. À cette fin, (nom de l'institution) mettra à leur disposition les ressources suivantes :

- Les documents normatifs en question ou des résumés (lister ces documents et indiquer où se les procurer)
- Du matériel pédagogique sur différents supports (décrire et indiquer où se procurer ce matériel)
- De l'accompagnement individuel de la part de votre gestionnaire
- Des cours formels sont aussi offerts. Veuillez consulter votre gestionnaire ou (autre source) pour plus de renseignements à propos de ces cours.

Les services de courriel, incluant la transmission et la réception des messages, l'information, les fichiers, les données et les métadonnées, doivent être utilisés aux fins des activités organisationnelles de (nom de l'institution) et non pas à des fins personnelles.



Le courriel ne peut être utilisé pour des activités illégales, contraires à l'éthique ou non professionnelles, ou pour réaliser un profit personnel.

Le courriel est la propriété de (nom de l'institution). Son utilisateur ne doit avoir aucune attente en matière de vie privée.

Un usage restreint du courriel est autorisé à des fins personnelles, à condition qu'il n'interfère pas avec le travail pour (nom de l'institution) et n'impose pas de charge excessive aux ressources technologiques.

Il est interdit, sauf autorisation écrite de (titre du poste), d'utiliser des services de courriel grand public (AOL, HotMail, Yahoo Mail, etc.) pour les activités organisationnelles de (nom de l'institution).

L'abonnement à des groupes de discussion ou à des listes de diffusion est interdit, à moins qu'il ne soit directement relié au travail pour (nom de l'institution).

L'utilisation du courriel pour proférer des menaces, faire du harcèlement ou véhiculer des propos désobligeants est strictement interdite et passible de mesures disciplinaires pouvant aller jusqu'au congédiement et pourrait entraîner des poursuites judiciaires. Un message répétitif et non désiré peut constituer du harcèlement. Tout employé recevant des courriels de cette nature devrait les sauvegarder dans un fichier à part et en transmettre une copie à (titre du poste) pour enquête.

Le système de courriel de (nom de l'institution) ne doit pas être utilisé pour faire circuler des blagues ou des chaînes de lettres. Les employés qui reçoivent de tels messages devraient en aviser (titre du poste).

Le (nom de l'institution) apporte régulièrement son soutien aux activités de (lister les organismes de bienfaisance ou autres : collectes de sang, campagnes de vaccination contre la grippe, Centraide, le Fonds Habineige, Toy Mountain, banques alimentaires, etc.). Le courriel est l'un des moyens de communication utilisés pour informer les employés et les inviter à contribuer financièrement à ces organismes ou à participer à leurs activités. Cependant, l'objectif premier du système de courriel est la réalisation des activités de (nom de l'institution); par conséquent, le système ne doit pas être utilisé pour promouvoir ou solliciter le soutien à une « bonne cause », autre que celles listées ci-haut, à moins d'avoir obtenu une autorisation préalable de (titre).

Les données, opinions ou déclarations produites par (nom de l'institution) ou lui appartenant ne doivent pas être diffusées à l'extérieur de l'institution sans l'autorisation préalable de (titre, suppléant, ou une personne désignée)

Les utilisateurs du courriel de (nom de l'institution) doivent savoir que les courriels non protégés peuvent être interceptés. Les utilisateurs devraient réfléchir au risque que représente l'envoi d'un message par courriel et recourir à d'autres moyens de communication, au besoin.

Il est impossible de prédire à quel moment l'institution pourrait être impliquée dans une poursuite judiciaire ou faire l'objet d'un audit, mais dans une telle éventualité, des courriels, dont certains sont considérés comme personnels par les utilisateurs, pourraient être exigés en preuve. Les utilisateurs qui écrivent des courriels et y joignent des documents doivent comprendre que cette information pourrait un jour être lue en cour à titre de preuve. Les messages devraient être rédigés dans un style professionnel et courtois. Le jargon et les expressions vulgaires sont à éviter.

Les utilisateurs devraient autant que possible éviter de joindre à leurs messages des documents lourds, tels que photographies, vidéo-clips ou fichiers audio. Les pièces de cette nature peuvent encombrer la boîte aux lettres du destinataire et l'empêcher de recevoir un message urgent ou important.

Les utilisateurs ne devraient pas diffuser largement des courriels à tout le monde sur le réseau. Seules certaines personnes autorisées peuvent le faire.

8.2. Responsabilités des administrateurs de réseaux ou de systèmes

Les administrateurs de réseaux devraient fournir l'infrastructure technique nécessaire à la gestion des courriels, concevoir et appliquer des procédures de sauvegarde et de récupération en cas de



sinistre, fournir des mécanismes de sécurité en TI et sur Internet à la fine pointe, contrôler et surveiller l'accès à l'information et aux documents.

Les administrateurs de réseaux devraient surveiller l'utilisation du courriel afin d'évaluer le respect des politiques et des Lignes directrices pour la gestion des courriels et, s'il y a lieu, enquêter lorsqu'il y a des soupçons d'utilisation abusive du courriel.

Les administrateurs de réseaux devraient créer, tenir à jour et conserver une documentation détaillée sur le système de courriel et les informations qu'il contient. Cette documentation devrait suffire à prouver l'authenticité et l'intégrité de tout courriel ou information associée, produit en preuve lors d'une action en justice.

Les administrateurs de réseaux devraient veiller à ce que les courriels relatifs aux activités organisationnelles ne soient pas stockés dans un dépôt non autorisé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les administrateurs de systèmes ont généralement pour mandat de veiller à la performance et à la rentabilité des systèmes de TI. Cet accent mis sur les TI peut entraîner des décisions et des actions contraires à une saine gestion des courriels en tant que document et source d'information. Par exemple, il pourrait sembler naturel à un administrateur de réseau de recommander l'élimination d'anciens documents afin d'améliorer l'efficacité du système de courriel. Cependant, une telle décision pourrait causer de sérieux problèmes à l'institution, en cas d'audit ou d'action en justice, si les documents éliminés doivent être produits en preuve.

À l'opposé, les gestionnaires de l'information savent très bien quels documents doivent être conservés, et pour combien de temps, mais se préoccupent peu des effets négatifs que la conservation de grandes quantités d'informations pourrait avoir sur la performance des systèmes opérationnels.

Bien que leurs mandats soient différents, les administrateurs de réseaux et les gestionnaires de l'information doivent travailler en collaboration et s'épauler mutuellement.

Les administrateurs de réseaux possèdent l'expertise requise pour concevoir l'infrastructure technique nécessaire à la gestion des courriels. Ils savent comment élaborer des procédures de sauvegarde et de récupération en cas de sinistre. Ils possèdent les outils permettant de régler avec précision les mécanismes de sécurité en TI, de contrôler et de surveiller l'accès aux documents et

à l'information conservée. Ils disposent aussi d'outils pour enquêter en cas de soupçons d'usage abusif du courriel.

Les administrateurs de réseaux sont capables de restreindre l'accès aux fichiers uniquement à ceux qui en ont besoin pour leur travail. Ils ont également la capacité, dans certaines circonstances bien définies, d'accéder au courriel d'un employé. Ce sera le cas, par exemple, s'il faut consulter rapidement une information contenue dans le courriel d'un employé, alors qu'il est absent, s'il faut diagnostiquer et régler un problème technique ou enquêter sur un possible usage abusif du courriel.

Si un courriel doit être produit en preuve lors d'une action en justice, l'administrateur de réseau doit pouvoir isoler l'information afin d'en empêcher la destruction, et d'en prouver l'authenticité et l'intégrité. Une telle preuve se fonde habituellement sur la documentation de système créée, tenue à jour et conservée par l'administrateur de système.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les administrateurs de réseaux et de systèmes devraient assumer les responsabilités suivantes relativement à la gestion des courriels :

- Fournir l'infrastructure technique nécessaire à la gestion des courriels
- Élaborer des procédures de sauvegarde et de récupération en cas de sinistre
- Améliorer constamment la sécurité des TI pour contrer l'arrivée de nouvelles menaces
- Contrôler et surveiller l'accès aux courriels et à l'information associée
- Apporter un soutien aux enquêtes reliées à de présumés usages abusifs du courriel
- Créer, fermer, geler ou suspendre les comptes de courriel
- Accéder au courriel d'un employé (dans certaines circonstances)
- Isoler l'information demandée dans le cadre d'actions en justice afin d'en empêcher la destruction
- Prouver l'authenticité et l'intégrité de courriels
- Créer, tenir à jour et conserver la documentation de système

8.3. Responsabilités des spécialistes en gestion de l'information

Les spécialistes en gestion de l'information assument généralement de très larges responsabilités et ne sont pas affectés exclusivement à la gestion des courriels. Cependant, ces responsabilités touchant la gestion de l'information en général, s'étendent bien entendu à la gestion des courriels.

Un spécialiste en gestion de l'information dirige et soutient une gestion de l'information efficace et efficiente au sein d'une organisation, à partir de la planification et du développement de systèmes jusqu'à l'élimination ou à la



conservation permanente des documents. (Paraphrase d'une définition sur le portail GI du gouvernement du Canada) :

(Source: http://www.informationmanagement.gc.ca/index_f.asp)

La Politique sur la gestion de l'information du Conseil du Trésor précise que les spécialistes en gestion de l'information – dont les bibliothécaires, les archivistes, les responsables de l'accès à l'information et de la protection des renseignements personnels, et les spécialistes en gestion des documents – contribuent à la gestion de l'information :

- (a) en fournissant conseils, outils, procédures, normes et lignes directrices conformes aux orientations formulées par le Secrétariat du Conseil du Trésor du Canada et Bibliothèque et Archives Canada;
- (b) en identifiant les besoins en matière d'information du personnel oeuvrant en technologie de l'information, afin de soutenir le développement et l'utilisation de procédures, systèmes, normes et outils en technologie de l'information;
- (c) en évaluant les besoins en matière de ressources et de formation en gestion de l'information.

(Source : http://www.tbs-sct.gc.ca/archives/ciopubs/mgih-grdg/2003/mgih-grdg1_f.asp)

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Le rôle du spécialiste en gestion de l'information varie selon la taille de l'organisation à laquelle il appartient, son expérience et son niveau d'autorité. Un spécialiste en gestion de l'information peut assumer quelques-unes ou l'ensemble des responsabilités suivantes :

- Fournir des programmes et des services en gestion de l'information et des documents concernant spécifiquement les courriels
- Saisir les courriels et l'information associée
- Organiser et décrire les courriels et l'information associée



- Créer, tenir à jour et appliquer des plans de classification, des notices descriptives et des métadonnées
- Fournir accès aux courriels et à l'information associée
- Stocker et protéger les courriels et l'information associée
- Disposer des courriels et de l'information associée
- Fournir des services électroniques pour la gestion des courriels

Les responsabilités du spécialiste en gestion de l'information peuvent entraîner certaines ou l'ensemble des tâches suivantes :

- Élaborer des plans ministériels en GI/TI relativement à la gestion des courriels
- Élaborer des politiques, normes et lignes directrices en GI/TI propres à la gestion des courriels
- Élaborer des méthodes de contrôle de la conformité en gestion des courriels
- Offrir des conseils en matière d'investissements en technologie de l'information et de stratégies de ressourcement en GI/TI pour la gestion des courriels
- Effectuer des vérifications de conformité en GI/TI (exercices de découverte et de disposition reliés aux courriels)
- Effectuer des analyses coûts/bénéfices et des analyses d'impact
- Planifier, concevoir et mettre en œuvre des stratégies de communication en matière de gestion des courriels
- Élaborer et diffuser des documents de communication relatifs à la gestion des courriels
- Promouvoir les services organisationnels sur Internet
- Gérer la structure de gouvernance du comité des GI/TI
- Participer aux groupes de travail interministériels sur les politiques, les normes et les lignes directrices en gestion de l'information

Dans les grandes institutions, il peut y avoir plusieurs spécialistes possédant une formation poussée et une longue expérience en gestion de l'information. Par contre, dans les petits organismes, les responsabilités du spécialiste en gestion de l'information sont parfois confiées à des personnes ayant peu de formation ou d'expérience pratique, ou assumant déjà d'autres responsabilités organisationnelles. Le but de la liste ci-dessus est de démontrer que la gestion de l'information est une tâche exigeante et complexe qui requiert l'allocation de ressources appropriées.



Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : l'institution offrira des programmes et services en gestion de l'information et des documents, qui apporteront un soutien efficace et efficient à la gestion des courriels. Ces programmes et services exigeront et soutiendront un certain nombre d'activités connexes :

- Saisir les courriels considérés comme information ou documents organisationnels
- Organiser et décrire les courriels considérés comme information ou documents organisationnels
- Créer, tenir à jour et appliquer des plans de classification
- Créer des notices descriptives et des métadonnées
- Fournir accès aux courriels considérés comme information ou documents organisationnels
- Stocker et protéger les courriels considérés comme information ou documents organisationnels
- Disposer des courriels considérés comme information ou documents organisationnels
- Fournir des services électroniques en gestion des courriels

8.4. Responsabilités des gestionnaires des opérations

Les gestionnaires devraient identifier les besoins des employés en matière de formation à la gestion des courriels et leur allouer du temps, pendant les heures de travail, pour leur permettre de suivre une formation appropriée.

Les gestionnaires devraient veiller à ce que le personnel se conforme aux présentes Lignes directrices pour la gestion des courriels, notamment les procédures de réception et de départ de même que les procédures d'orientation et de départ à classification et le stockage adéquats des documents et de l'information, et l'application de délais de conservation appropriés.

Les gestionnaires devraient s'assurer que les employés aient à leur disposition tous les documents de référence concernant la gestion des courriels, ou qu'ils sachent où et comment les obtenir au besoin.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation

Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants
--------------	---	--	------------------------------	------------



Justification

Les gestionnaires sont normalement responsables d'identifier toute formation dont leurs employés pourraient avoir besoin, sur tout sujet associé à leur travail, et d'allouer du temps, pendant les heures de bureau, pour donner cette formation.

Les gestionnaires sont normalement responsables de superviser le travail de leurs employés, notamment la qualité et la pertinence du travail accompli, l'utilisation efficace des outils à leur disposition, l'exactitude et l'exhaustivité des documents qu'ils conservent.

Les gestionnaires peuvent aussi participer à l'établissement des exigences en matière de conservation et d'élimination des documents, en général – mais pas toujours – sur avis des spécialistes en gestion de l'information. Les gestionnaires peuvent aussi participer à la mise en place du système de classement pour le stockage des courriels et de leurs pièces jointes. Les gestionnaires doivent également faire connaître ces exigences aux employés sous leur supervision.

Ces responsabilités comprennent la supervision et la gestion de l'utilisation que font les employés de leur courriel.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les gestionnaires devraient assumer les responsabilités suivantes en matière de gestion des courriels :

- Identifier les besoins des employés en matière de formation à la gestion des courriels
- Allouer du temps, pendant les heures de travail, pour permettre aux employés de suivre une formation appropriée
- Veiller à ce que le personnel se conforme aux politiques et lignes directrices en gestion des courriels
- Veiller à ce que les employés utilisent un mode de classification et de stockage approprié pour leurs courriels
- Veiller à ce que des délais de conservation appropriés soient appliqués aux courriels
- Veiller à ce que les employés aient accès à des documents de référence sur la gestion des courriels
- Établir le système de classement pour le stockage des courriels et de leurs pièces jointes
- Superviser et gérer l'utilisation du courriel par le personnel



8.5. Responsabilités des dirigeants

Les dirigeants devraient définir les orientations stratégiques en matière de courriel, et guider l'élaboration et l'adoption d'une politique institutionnelle sur la gestion des courriels.

Un dirigeant qui assume également le rôle de gardien des documents devrait veiller à ce que les courriels faisant l'objet de demandes en vertu de lois d'accès ou dans le cadre d'actions en justice ne soient pas détruits.

Les dirigeants devraient accorder un financement adéquat aux programmes et systèmes de gestion des courriels, afin de garantir leur conformité aux politiques et lois en vigueur, et aux présentes Lignes directrices et recommandations pour la gestion des courriels.

Les dirigeants devraient s'assurer que de bonnes formations en gestion des courriels soient préparées et offertes aux employés, que la participation des employés soit consignée et l'information conservée, et que le matériel pédagogique et de référence soit disponible sur différents supports.

Les dirigeants doivent s'assurer que les employés reçoivent les présentes Lignes directrices pour la gestion des courriels et les recommandations associées, et que ceux-ci confirment par écrit les avoir bien reçues et comprises; cette confirmation écrite sera conservée par la suite.

Les dirigeants devraient réexaminer régulièrement les politiques et procédures en matière de gestion des courriels, afin d'en évaluer l'efficacité, résoudre les éventuels problèmes et apporter des améliorations.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Justification

Les institutions, et par conséquent leurs dirigeants, sont responsables des actions de leurs employés, incluant la gestion, la conservation et l'élimination des courriels de manière appropriée.

La gestion des courriels est devenue l'un des plus redoutables défis à relever par les institutions en matière de gestion de l'information; elle mérite donc que les dirigeants s'y intéressent de près.



Les dirigeants sont généralement responsables de définir les orientations stratégiques et les politiques de leur institution et de veiller à ce que des ressources adéquates soient allouées à ses différentes activités, ainsi qu'à la création et à la conservation de l'information et des documents gouvernementaux. En général, les dirigeants sont aussi responsables de l'allocation des fonds pour la formation du personnel.

Exemple d'énoncé de politique

Si la présente recommandation est appropriée aux circonstances, il est suggéré d'adopter l'énoncé de politique suivant.

Si ce n'est pas le cas, veuillez préciser une autre façon de procéder.

(Nom de l'institution) adopte la politique suivante : les dirigeants devraient assumer les responsabilités suivantes en matière de gestion des courriels :

- Définir les orientations stratégiques concernant la gestion des courriels
- Guider l'élaboration et l'adoption d'une politique sur la gestion des courriels
- Veiller à ce que les courriels pouvant faire l'objet de demandes de consultation en vertu de lois d'accès ou dans le cadre d'actions en justice ne soient pas détruits
- Allouer des fonds suffisants aux programmes et systèmes de gestion des courriels
- Veiller à ce que de bonnes formations en gestion des courriels soient préparées et offertes aux employés
- Veiller à ce que la participation des employés soit consignée et l'information conservée
- Veiller à ce que le matériel pédagogique et de référence soit disponible sur différents supports
- Veiller à ce que les employés reçoivent les politiques et lignes directrices en gestion des courriels
- Veiller à ce que les employés confirment par écrit avoir bien reçu et compris ces documents et que cette confirmation écrite soit conservée par la suite
- Assumer la responsabilité des actions de leurs employés, incluant la gestion, la conservation et l'élimination des courriels de manière appropriée



ANNEXE A. RÔLES ET RESPONSABILITÉS

Le tableau ci-dessous illustre le partage des responsabilités entre les divers intervenants, dans la mise en oeuvre des présentes Lignes directrices pour la gestion des courriels et des recommandations associées.

- Les utilisateurs (UTIL)
- Les administrateurs de systèmes ou de réseaux (ASYS)
- Les spécialistes en gestion de l'information (SGI)
- Les gestionnaires des opérations (GOP)
- Les dirigeants (DIR)

La responsabilité est indiquée par un crochet à l'intersection d'un intervenant et d'une ligne directrice ou d'une recommandation.

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
0. Introduction au Lignes directrices pour la gestion des courriels					
0.2. Lignes directrices	✓	✓	✓	✓	✓
0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde?	✓	✓	✓	✓	✓
0.4. Quels sont les résultats attendus?	✓	✓	✓	✓	✓
0.5. Pourquoi la gestion des courriels est-elle si importante?	✓	✓	✓	✓	✓
0.6. Domaines où les lignes directrices ne s'appliquent pas	✓	✓	✓	✓	✓
0.7. Feuille de route pour se conformer aux lignes directrices	✓	✓	✓	✓	✓
0.8. Cycle de vie de l'information électronique	✓	✓	✓	✓	✓
0.9. Définitions	✓	✓	✓	✓	✓
1. Les institutions doivent se doter d'un plan pour gérer les courriels					
1.0. Recommandations					
1.1. Gérer les programmes et les systèmes de courriel de manière intégrée	✓	✓	✓		
1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels					✓



Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels					✓
1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées ont bien été distribuées, lues et comprises					✓
1.5. Conserver des dossiers sur les activités de formation et sur la participation					✓
2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles					
2.0. Recommandations					
2.1. Créer, expédier et stocker les courriels de manière structurée	✓	✓	✓		
2.2. Recevoir et stocker les courriels de manière structurée	✓	✓	✓		
2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière	✓				
2.4. Garder un seul exemplaire de chaque courriel	✓	✓	✓	✓	✓
2.5. Gérer et conserver les pièces jointes aux courriels		✓	✓		
2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada	✓	✓	✓	✓	✓
2.7. Utiliser avec modération les listes de diffusion institutionnelles	✓				
2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource		✓	✓		
2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu	✓	✓		✓	✓
2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu	✓	✓			✓
2.11. Éviter d'utiliser la fonction "Répondre à tous"	✓				
3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles					
3.0. Recommandations					



Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels	✓	✓	✓		
3.2. Déterminer où classer la « copie officielle »		✓	✓		✓
3.3. Conserver les métadonnées associées aux courriels		✓	✓		
3.4. Classifier et classer les courriels systématiquement et fréquemment	✓				
3.5. Gérer le stockage en ligne temporaire des courriels	✓	✓			
3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels	✓	✓	✓	✓	
3.7. Limiter le contenu des courriels à un seul sujet	✓				
3.8. Décrire l'objet d'un courriel en termes clairs et significatifs	✓				
3.9. Prévoir un système d'indexation des courriels		✓	✓		
3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (<i>threading</i>)		✓	✓		
4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels					
4.0. Recommandations					
4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur	✓				
4.2. Utiliser les journaux d'exploitation pour constituer une piste de vérification et veiller au respect des règles		✓	✓		
4.3. Afficher les noms dans les en-têtes et les adresses de courriel		✓			
4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique		✓	✓		
4.5. Surveiller la performance des activités de découverte et de disposition des courriels		✓	✓	✓	



Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés					
5.0. Recommandations					
5.1 Éviter de procéder à des purges indiscriminées dans les systèmes de courriels		✓			
5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées	✓	✓		✓	
5.3. Enlever le chiffrement avant de quitter une institution	✓				
5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada		✓	✓		
5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel		✓			
5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets	✓	✓			
5.7. Protéger les systèmes contre les pertes et les dommages		✓	✓		
5.8. Employer le bon niveau de classification de sécurité				✓	✓
5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun	✓	✓		✓	
5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel	✓	✓			
5.11. Utiliser des mesures de protection et d'authentification des messages		✓			
5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre		✓			
5.13. Utiliser la signature numérique s'il y a lieu	✓	✓	✓	✓	✓
5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada		✓	✓		
5.15. Ne pas employer de signature numérisée pour signer un courriel	✓				
5.16. Utiliser le chiffrement s'il y a lieu	✓	✓	✓	✓	✓



Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
5.17. Employer le stockage de proximité pour la conservation à long terme des courriels		✓	✓		
5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore	✓	✓	✓		
5.19. Protéger les courriels en protégeant les supports de conservation		✓	✓		
5.20. Protéger les courriels de l'obsolescence		✓	✓		
5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel		✓			
5.22. Conserver en permanence la documentation du système de courriel		✓	✓		
5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes		✓	✓		
5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document	✓	✓	✓		
6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes					
6.0. Recommandations					
6.1. Obtenir une autorisation de disposition des courriels	✓	✓	✓		
6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun		✓	✓		
6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP		✓	✓		
7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin					
7.0. Recommandations					
7.1. Évaluer l'efficacité de la gestion des courriels			✓		



Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels					
8.0. Recommandations					
8.1. Responsabilités des utilisateurs	✓				
8.2. Responsabilités des administrateurs de réseaux ou de systèmes		✓			
8.3. Responsabilités des spécialistes en gestion de l'information			✓		
8.4. Responsabilités des gestionnaires des opérations				✓	
8.5. Responsabilités des dirigeants					✓



ANNEXE B. RESPECT DES LIGNES DIRECTRICES POUR LA GESTION DES COURRIELS ET PLAN DE MISE EN OEUVRE

Importance des retombées (types de retombées ou secteurs touchés)

Meilleure capacité de se conformer aux exigences légales

- Prévient la modification ou la perte de documents
- Prévient une exposition inutile de l'institution à des actions en justice

Réduction du nombre d'exemplaires d'un courriel

- Simplifie la récupération des fichiers lors d'un audit, d'une action en justice ou d'une demande d'accès à l'information
- Simplifie l'élimination des documents en réduisant le nombre d'exemplaires

Documentation et conservation de la documentation

- La documentation des systèmes de gestion des courriels devra être très détaillée (probablement encore plus qu'elle ne l'est actuellement).
- La documentation devra être conservée à long terme dans l'éventualité où elle pourrait être requise pour établir la fiabilité et l'intégrité du système aux fins d'un audit ou d'une action en justice.

Obsolescence

- Les institutions sont tenues de garantir que les courriels demeurent lisibles pendant toute la durée de leur délai de conservation. À cette fin, elles doivent veiller à conserver les logiciels et les systèmes capables de lire les courriels, ou à faire migrer les courriels vers un format lisible par les technologies les plus récentes, ou encore à s'assurer que toute technologie acquise possède une compatibilité ascendante.

Temps alloué par les utilisateurs à la gestion des courriels

- Une partie du temps de travail des utilisateurs devra être consacrée à la gestion des courriels – et il se peut que cette partie soit plus importante qu'elle ne l'est actuellement.

Élimination au moment opportun

- Une gestion efficace et efficiente des courriels facilitera le repérage des documents et de l'information, et leur élimination au moment opportun, à l'expiration de leur délai de conservation.

Formation

- De nouveaux programmes de formation améliorés seront mis en place, dont certains s'adresseront à l'ensemble des utilisateurs. Ces programmes nécessiteront la conception d'outils pédagogiques sur différents supports, ceci afin de servir d'aide-mémoire et d'offrir aux participants la possibilité de choisir le mode d'apprentissage qui leur convient le mieux. Comme les exigences organisationnelles varient d'une institution à l'autre, les formations devront probablement être adaptées dans une certaine mesure. Cette adaptation demandera temps et effort de la part des concepteurs, des formateurs et des participants.
- Des formations plus spécialisées devront être conçues à l'intention des dirigeants, des spécialistes en gestion de l'information, des administrateurs de systèmes et des gestionnaires des opérations. Cela exigera une fois de plus des efforts particuliers de la part des spécialistes tels que les concepteurs et les formateurs, et de la disponibilité de la part des participants.

Temps consacré à la gestion (gestionnaire des opérations)

Le gestionnaire devra consacrer une partie de son temps à identifier les besoins en matière de formation, à guider le personnel et à veiller au respect des règles.

Stockage

- Il faudra sauvegarder les courriels, métadonnées et pièces jointes qui sont considérés comme de l'information ou des documents officiels.
- Il faudra mettre en place une infrastructure pour stocker les courriels qui sont considérés comme de l'information ou des documents officiels.
- Il faudra organiser le stockage afin de permettre une récupération et une utilisation efficaces et efficientes des courriels qui sont considérés comme de l'information ou des documents officiels et d'en faciliter plus tard l'élimination.

Coût

La gestion des courriels engendrera des coûts à tous les niveaux et dans tous les secteurs de l'institution.

Secteurs où l'on peut prévoir une augmentation des coûts

Ressources humaines

La gestion des courriels exigera un effort particulier de la part de tous les employés, contractuels et autres utilisateurs du courriel dans chacun des ministères et organismes gouvernementaux.

- Les utilisateurs devront consacrer du temps à gérer leurs courriels. Ils auront à identifier les courriels qui ne constituent pas des documents gouvernementaux et les supprimer. Ils devront décider comment classifier leurs courriels et les ranger, avec les métadonnées et pièces jointes dans des zones de stockage désignées et approuvées par l'organisation.
- Les administrateurs de systèmes et de réseaux devront consacrer du temps et des efforts à concevoir, opérer et tenir à jour l'infrastructure technique nécessaire à la gestion des courriels.
- En plus de leurs tâches habituelles, les gestionnaires des opérations devront réserver du temps pour identifier les besoins des employés en matière de formation à la gestion des courriels, et veiller à ce que ces besoins soient satisfaits. Les gestionnaires devront également veiller à ce que les employés respectent les présentes lignes directrices et les politiques associées, afin qu'ils utilisent des modes de classification et de stockage appropriés aux courriels. De plus, les gestionnaires devront veiller à l'application de bons délais de conservation aux courriels.
- Les spécialistes en gestion de l'information peuvent s'attendre à devoir consacrer du temps à l'élaboration de plans de classification et à conseiller les gestionnaires sur la manière de concevoir un système de classement pour le stockage des courriels et de leurs pièces jointes. Ils auront aussi à collaborer avec les administrateurs de systèmes à la conception de l'infrastructure pour la gestion des courriels.
- Les dirigeants devront aussi consacrer des énergies à la gestion des courriels. Leur rôle consistera à établir des orientations stratégiques en ce domaine, et à guider l'élaboration et l'adoption d'une politique relative à la gestion des courriels. Les dirigeants devront également revoir les budgets et accorder un financement adéquat aux programmes et systèmes de gestion des courriels, et veiller à ce que des formations de qualité soient préparées et offertes aux employés en matière de gestion des courriels.
- Les spécialistes en formation devront concevoir des documents pédagogiques appropriés et offrir des programmes de formation en soutien à la gestion des courriels.

Technologie

Une gestion efficace des courriels exigera peut-être une certaine adaptation de l'infrastructure actuelle ou la mise en place d'une nouvelle infrastructure. Le développement et la maintenance de cette infrastructure engendreront probablement des coûts supplémentaires. De plus, il faudra se procurer des logiciels, des équipements et des installations de stockage spécialisés.



Domaines où il sera possible d'économiser ou d'éviter des coûts

C'est surtout en matière de respect des lois qu'il sera possible d'éviter des coûts. En effet, la capacité de stocker, de conserver et de récupérer les courriels et l'information associée, de manière fiable et efficiente, permettra de réduire substantiellement les coûts de recherche lors d'une action en justice, d'un audit ou d'une demande d'accès à l'information.

Les risques associés à la fiabilité de la preuve légale seront également réduits grâce à la capacité d'éliminer les courriels et l'information associée, de manière efficace et efficiente, au moment opportun, parfois à l'expiration d'un délai obligatoire.

Une gestion efficace des courriels apportera aussi des bénéfices immatériels en procurant un accès continu à la mémoire institutionnelle, en évitant de refaire les mêmes tâches et en offrant la possibilité de réutiliser l'information.

Portée – secteurs d'activités touchés

Pratiquement toutes les activités du gouvernement canadien seront touchées par ce projet.

Lois nécessitant ces lignes directrices

Les lois listées ci-dessous ne prescrivent pas expressément une norme ou des lignes directrices particulières en matière de gestion des courriels; elles établissent toutefois certaines responsabilités et obligations légales relatives à la divulgation (et à la non-divulgation), et à l'élimination de l'information, incluant l'information électronique. Cette dernière comprend ou peut être interprétée comme comprenant les courriels, leurs métadonnées et pièces jointes.

Les courriels font partie des informations les plus fréquemment demandées lors d'une action en justice, d'un audit ou d'une demande d'accès à l'information.

Les institutions du gouvernement canadien ne sont pas tenues de documenter leur processus décisionnel ou leurs actions, à l'exception des transactions financières. Cependant, si de telles informations sont recueillies par une institution, celle-ci doit en assurer la conservation durant une période de temps appropriée.

Les présentes lignes directrices sont conçues pour faciliter le respect des obligations et responsabilités imposées en vertu des lois suivantes (on trouvera à l'annexe C la description de ces lois et les adresses Internet où on peut les trouver).

- Accès à l'information, Loi sur l'



- Bibliothèque et les Archives du Canada, Loi sur la
- Charte canadienne des droits et libertés
- Crédits, Lois de
- Droit d'auteur, Loi sur le
- Emploi dans la fonction publique, Loi sur l'
- Gestion des finances publiques, Loi sur la
- Langues officielles, Loi sur les
- Preuve au Canada, Loi sur la
- Protection civile, Loi sur la
- Protection de l'information, Loi sur la
- Protection des renseignements personnels et les documents électroniques, Loi sur la
- Protection des renseignements personnels et règlements afférents, Loi sur la
- Responsabilité civile de l'État et le contentieux administratif, Loi sur la
- Service canadien de renseignement de sécurité, Loi sur le
- Statistique, Loi sur la
- Vérificateur général, Loi sur le

Politiques fédérales nécessitant ces lignes directrices

Politique sur la gestion de l'information

L'objectif de la présente Politique est d'assurer une gestion de l'information efficace à l'appui de la mise en œuvre des programmes et des services; d'assurer des processus décisionnels efficaces; de faciliter la reddition des comptes, la transparence et la collaboration; de préserver l'information et de veiller à l'accès à l'information et aux documents pour le bienfait de la génération actuelle et des générations à venir.

Résultats escomptés

- Les programmes et services du gouvernement permettent un accès pratique à de l'information pertinente, fiable, intégrale et à propos.
- L'information et les documents sont gérés comme des ressources précieuses pour appuyer les résultats des programmes et des services, ainsi que pour satisfaire aux besoins opérationnels et aux obligations de rendre des comptes.
- Des structures, des mécanismes et des ressources de gouvernance sont en place pour assurer une gestion de l'information continue et efficace.



(Source: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/pim-pgi01_f.asp)

Plusieurs autres politiques nécessitent le recours aux présentes Lignes directrices, ou imposent elles-mêmes des normes ou des lignes directrices en matière de gestion des courriels.

- Accès à l'information, Politique sur l'
- Apprentissage, de formation et de perfectionnement, Politique en matière d'
- Autorisation et l'authentification électroniques, Politique sur l'
- Communication, Politique de
- Évaluation, Politique d'
- Évaluation des facteurs relatifs à la vie privée, Politique d'
- Gestion de l'information, Politique sur la
- Gestion de l'infrastructure à clé publique, Politique de
- Gestion des projets, Politique sur la
- Gestion des risques, Politique sur la
- Gestion des technologies de l'information, Politique sur la
- Protection des renseignements personnels, Politique sur la
- Sécurité, Politique sur la
- Services communs, Politique sur les
- Utilisation des réseaux électroniques, Politique d'

Mécanismes de surveillance et de vérification de la conformité

Il existe différents moyens de surveiller et de vérifier le respect des politiques. Par exemple, on peut procéder à des vérifications manuelles et à des exercices de découverte informatique, ou utiliser des journaux d'exploitation pour obtenir des réponses aux questions suivantes :

POLITIQUE ET GOUVERNANCE

- Y a-t-il une politique concernant les Lignes directrices pour la gestion des courriels?
- Cette politique couvre-t-elle l'ensemble des Lignes directrices pour la gestion des courriels et des recommandations associées, et indique-t-elle pour chacune si elle s'applique ou non?
- Lorsque certaines lignes directrices ou recommandations sont sujettes à interprétation, la politique précise-t-elle comment les appliquer?



- Quant aux lignes directrices et recommandations applicables à l'institution, la politique indique-t-elle comment les interpréter et les appliquer?
- La politique est-elle distribuée par la direction et celle-ci en fait-elle la promotion?
- La politique a-t-elle été reçue, lue et comprise par le personnel?
- Y a-t-il un promoteur parmi les dirigeants et un comité directeur responsables et imputables de la gestion de l'information en général, et plus particulièrement de la gestion des courriels?
- Y a-t-il un plan pour l'amélioration de la gestion des courriels, et l'institution suit-elle ce plan?

PROGRAMME DE SENSIBILISATION ET DE FORMATION À LA GESTION DES COURRIELS

- Y a-t-il un programme de sensibilisation de haut niveau à l'intention du personnel?
- L'efficacité de ce programme est-elle évaluée?
- Y a-t-il des programmes de formation portant spécifiquement sur la gestion des courriels et sur les rôles et responsabilités des dirigeants, des spécialistes en gestion de l'information, des administrateurs de systèmes et de réseaux, des gestionnaires des opérations et des utilisateurs?
- Les nouveaux employés reçoivent-ils une formation en gestion des courriels?
- Une formation en gestion des courriels est-elle offerte au personnel déjà en place?

ÉVALUATION DE LA CONFORMITÉ

- Y a-t-il un programme servant à évaluer dans quelle mesure les utilisateurs respectent les normes?
- Existe-t-il des paramètres et des cibles permettant d'évaluer dans quelle mesure un utilisateur se conforme à une norme en particulier?
- Y a-t-il des normes comparatives pour les paramètres en gestion des courriels et existe-t-il des cibles, des plans et des activités en place pour rehausser le niveau de conformité?
- Le respect des Lignes directrices pour la gestion des courriels et des recommandations associées est-il vérifié régulièrement et des mesures correctrices sont-elles apportées dans les cas de non-respect par les utilisateurs?
Si oui, l'efficacité de ces mesures est-elle évaluée?
- Les dépenses en gestion de l'information et en gestion des courriels sont-elles proportionnelles à la taille de l'organisation?

CYCLE DE VIE DE L'INFORMATION ÉLECTRONIQUE

- Y a-t-il des délais de conservation établis pour différents types de documents et d'information?
- Existe-t-il des mesures de protection contre l'obsolescence?
- Les courriels et l'information associée sont-ils adéquatement protégés et conservés?
- La documentation du système de gestion des courriels est-elle à jour et conservée comme un document permanent?
- La documentation de système peut-elle soutenir l'admissibilité en preuve des courriels, conformément aux règles de la preuve?
- Les courriels sont-ils conservés avec leurs métadonnées et pièces jointes, et sinon, leur relation est-elle préservée?

Bien entendu, la liste de questions ci-dessus n'est pas exhaustive; il pourrait être souhaitable de poser d'autres questions et de mesurer d'autres éléments de conformité.

Public cible et intervenants

Les dirigeants constituent un public cible parce qu'ils sont responsables de la conservation de l'information et des documents gouvernementaux, ainsi que des gestes posés par leurs employés. Il s'agit aussi d'un nouveau public cible en ce qui concerne la promotion de la gestion de l'information (GI), celle-ci étant habituellement confiée aux professionnels en GI. C'est qu'on reconnaît de plus en plus que la gestion de l'information a besoin d'un meilleur financement pour répondre aux exigences des lois, des tribunaux et des vérificateurs du gouvernement fédéral. Il est donc essentiel que le message sur l'importance de financer adéquatement et de promouvoir la gestion de l'information soit porté par la direction de l'institution.

Les professionnels en gestion de l'information constituent le public cible traditionnel pour les normes, lignes directrices, pratiques et outils reliés à la GI. Cependant, ce groupe n'est pas homogène; les grandes institutions ont la capacité d'engager du personnel hautement qualifié et expérimenté, mais dans les petites organisations, les responsables de la GI ont parfois très peu de formation et d'expérience dans le domaine.

Les administrateurs de systèmes ont la responsabilité de mettre en place, de faire fonctionner et de tenir à jour l'infrastructure qui soutient le courriel et la gestion des courriels. Ces personnes doivent connaître et comprendre les Lignes directrices pour la gestion des courriels, afin de pouvoir travailler efficacement avec les gestionnaires de l'information.

Les gestionnaires des opérations sont en contact direct avec les utilisateurs et sont les mieux placés pour veiller au respect des normes, appliquer des mesures correctrices, évaluer les besoins en matière de formation et obtenir de la formation pour leur personnel. Le gestionnaire des



opérations peut aussi travailler en collaboration avec le gestionnaire de l'information et l'administrateur de systèmes pour concilier les exigences et les contraintes relatives à la gestion de l'information organisationnelle; il devrait donc connaître et comprendre les présentes Lignes directrices.

Les utilisateurs sont sur la ligne de front en ce qui concerne la gestion des courriels. Ils devront prendre eux-mêmes la décision de conserver ou de supprimer leurs messages; ils devront aussi classer et stocker ces messages. Les utilisateurs sont le premier maillon de la chaîne que constitue le processus de gestion des courriels.

Les formateurs devront connaître et comprendre les présentes Lignes directrices pour la gestion des courriels, ou à tout le moins les lignes directrices et les recommandations destinées au public cible pour lequel ils préparent du matériel pédagogique, conçoivent ou offrent des programmes de formation.

Stratégie de mise en œuvre recommandée

Il est recommandé de mettre en œuvre ces nouvelles lignes directrices pour la gestion des courriels dans un délai d'un an suivant leur approbation.

Les dirigeants, les spécialistes en gestion de l'information et les administrateurs de systèmes doivent être prêts à intervenir, et ce, avant les utilisateurs. Les dirigeants seront sensibilisés en priorité; ils devront être convaincus des avantages de la gestion des courriels et en promouvoir la mise en œuvre. Ce sont les dirigeants qui devront être motivés à réaffecter des fonds provenant de ressources existantes, et veiller à ce que des politiques soient rédigées afin de guider la mise en œuvre des présentes lignes directrices dans leur organisation. Ce sont eux qui autoriseront l'élaboration de procédures et de programmes de formation. Ce sont également eux qui autoriseront les changements à effectuer à l'infrastructure technologique, afin que tout soit prêt pour la mise en œuvre des présentes Lignes directrices.

Les gestionnaires de l'information et les administrateurs de systèmes devront travailler en étroite collaboration, possiblement avec une plus large contribution de spécialistes en technologie de l'information ou de consultants externes pour concevoir et effectuer tous les changements jugés nécessaires aux applications informatiques ou à l'infrastructure technologique soutenant la gestion des courriels. L'élaboration d'une campagne de sensibilisation, ainsi que de documents pédagogiques et de programmes de formation pourra débuter une fois finalisées la politique et la conception informatique. Il faudra probablement apporter certains ajustements à ces documents lorsque la période d'essai et de débogage sera terminée.



Un programme de surveillance de la conformité devrait démarrer immédiatement après la mise en œuvre et se composer d'un mélange équilibré de soutien technologique et d'interventions humaines.

LES TROIS PREMIERS MOIS (L'ÉCHÉANCIER PEUT VARIER D'UNE INSTITUTION À L'AUTRE)

- Début de la publication des Lignes directrices pour la gestion des courriels, laquelle se poursuivra pendant deux ans.
- Sensibilisation des dirigeants, des spécialistes en gestion de l'information et des administrateurs de systèmes
- Identification des étapes de mise en œuvre des Lignes directrices
- Réaffectation des fonds à l'intérieur des budgets existants afin d'entreprendre les travaux préparatoires

DE TROIS À SIX MOIS

- Préparation, par les institutions, de politiques et de procédures en gestion des courriels, identification et planification des modifications éventuelles à apporter à l'infrastructure

DE SIX À NEUF MOIS

- Modification et mise à l'essai de l'infrastructure (gestion des courriels, sécurité, récupération en cas de sinistre)
- Mise à l'essai et finalisation des procédures
- Préparation et mise à l'essai de plans de surveillance de la conformité
- Élaboration de documents pédagogiques concernant la politique, les procédures et l'infrastructure en gestion des courriels

DE NEUF À DOUZE MOIS

- Démarrage d'un vaste programme de sensibilisation à la gestion des courriels, afin de préparer les utilisateurs à la mise en œuvre des Lignes directrices
- Début des formations destinées à préparer les employés, contractuels et autres utilisateurs à la mise en œuvre des Lignes directrices

APRÈS DOUZE MOIS

- Fin de la mise en œuvre des Lignes directrices
- Début de la surveillance de la conformité
- Identification et réparation des bogues initiaux

Exigences en matière de surveillance et facteurs de succès

La surveillance de la conformité en gestion des courriels nécessitera l'établissement de paramètres, lesquels pourront varier d'une institution à l'autre, selon les exigences organisationnelles de chacune et sa façon d'interpréter et de mettre en œuvre les Lignes directrices.

Cette surveillance devra être effectuée régulièrement. Il faudra sans doute procéder assez fréquemment durant la période d'introduction des Lignes directrices, puis moins souvent lorsque celles-ci seront bien intégrées dans l'infrastructure et les pratiques courantes de l'organisation.

Le succès d'un programme de gestion des courriels dépendra largement de l'impulsion donnée par le dirigeant qui s'en fera le promoteur. Cette personne devra avoir l'autorité nécessaire pour allouer des fonds au programme, être disposée à participer à l'établissement de cibles de conformité et prendre la responsabilité de diriger l'institution vers l'atteinte de ces cibles.

Procédures et mécanismes de surveillance

Les journaux d'exploitation fournissent une quantité considérable de données qui peuvent être synthétisées dans des rapports relatifs à une large gamme de paramètres en gestion des courriels.

Les gestionnaires des opérations peuvent, périodiquement, effectuer des vérifications à l'ordinateur de leurs employés, afin de voir si ces derniers ont correctement classé et stocké leurs courriels, plutôt que de les accumuler dans la boîte « Réception » ou « Messages envoyés ».

Les exercices de découverte électronique (ou les simulations d'audit ou de demandes d'accès à l'information) aident à identifier les problèmes de conformité aux lignes directrices, en vérifiant la capacité de l'institution à repérer et à récupérer l'information électronique, incluant les courriels.

Les vérifications de conformité peuvent établir le degré de conformité en posant des questions toutes simples, par exemple, s'il y a une politique sur la gestion des courriels et s'il y a des programmes de formation en la matière. Une vérification de conformité pourrait aussi inventorier les caractéristiques actives de la technologie utilisée pour gérer les courriels.



Consensus atteint par le Groupe de travail sur les lignes directrices

Après s'être réuni plusieurs fois à Ottawa, en février et en mars 2006, le Groupe de travail en est arrivé à un large consensus. Ce groupe était composé de représentants de quatre ministères du gouvernement fédéral :

- Santé Canada
- Affaires indiennes et du Nord Canada
- Travaux publics et Services gouvernementaux Canada
- Anciens combattants Canada

Lors de ces réunions, une première version de ce qui est maintenant appelé « Lignes directrices pour la gestion des courriels – Feuille de route » a été révisée attentivement, et largement discutée. De ces discussions ont émergé d'intéressantes suggestions concernant la structuration du document, le contenu général de plusieurs lignes directrices, les exemples d'énoncés de politique et, dans bien des cas, la terminologie précise à utiliser. La plupart des participants (tous, dans plusieurs cas) se sont ralliés à ces suggestions, lesquelles ont été prises en considération dans les versions subséquentes du document.

Contribution des réviseurs

Au cours des mois de janvier et de février 2008, le document de travail « Lignes directrices pour la gestion des courriels – Feuille de route » a été revu en détail par des spécialistes en gestion de l'information, représentant plusieurs ministères et organismes gouvernementaux.

- Gouvernement du Canada
 - Agence de promotion économique du Canada atlantique
 - Agence du revenu du Canada
 - Citoyenneté et Immigration Canada
 - Bibliothèque et Archives Canada
 - Commissariat à la protection de la vie privée du Canada
 - Gendarmerie royale du Canada
 - Transports Canada
- Gouvernement de l'Alberta
 - Services Alberta

Une fois de plus, un large consensus a été atteint en faveur du document et de son contenu. L'exercice a cependant, comme la fois précédente, généré plusieurs suggestions très pertinentes à



propos de la structuration du document, du contenu de plusieurs lignes directrices, des exemples d'énoncés de politique et, dans bien des cas, de la terminologie précise à utiliser.

Quelques participants se sont demandé s'il ne faudrait pas considérer globalement la question de la gestion de l'information gouvernementale, plutôt que de s'intéresser uniquement aux courriels. Cette idée, exprimée par une minorité de spécialistes, n'a pas été discutée plus longuement, car on a estimé qu'elle dépassait largement la portée de l'exercice.

Enjeux majeurs non résolus

Les agendas, les listes de personnes-ressources et les listes de tâches font généralement partie des logiciels de courriels les plus utilisés actuellement. Ces fonctionnalités n'ont cependant pas été considérées dans l'étude qui a mené à l'élaboration des présentes Lignes directrices. Ce document ne traite pas non plus de l'usage envahissant des appareils mobiles, de l'avènement de la messagerie instantanée et d'autres avancées récentes en matière d'évolution et de convergence des technologies.

Lignes directrices pour la gestion des courriels – estimation des principaux coûts de mise en œuvre

Le tableau qui suit vise à aider les institutions de différentes tailles à estimer les principaux coûts de mise en œuvre, par ordre d'importance. Les domaines les plus susceptibles d'engendrer des coûts sont indiqués par un signe de dollar (\$). Les coûts peuvent être calculés en dollars, en Équivalents temps plein (ETP) ou par tout autre moyen jugé approprié par l'institution. Les signes de dollars sont seulement suggérés. En revanche, les estimateurs ne sont pas obligés d'indiquer les coûts dans les zones identifiées par un signe de dollar et rien ne les empêche d'inscrire les coûts dans les cases ne comprenant pas de signes de dollars.



Tableau d'estimation des coûts de mise en œuvre des Lignes directrices pour la gestion des courriels

Les trois premiers mois

Tâches	Conception et élaboration	Temps des formateurs et des participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Début de la publication des Lignes directrices pour la gestion des courriels, laquelle se poursuivra pendant deux ans	\$					
Sensibilisation des dirigeants, des spécialistes en gestion de l'information et des administrateurs de systèmes	\$	\$				
Identification des étapes de mise en œuvre des Lignes directrices	\$					
Réallocation des fonds à l'intérieur des budgets existants afin d'entreprendre les travaux préparatoires	\$					

De trois à six mois

Tâches	Conception et élaboration	Temps des formateurs et des participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Préparation de politiques	\$					



Tâches	Conception et élaboration	Temps des formateurs et des participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Élaboration de procédures pour la gestion des courriels	\$					
Identification et planification des modifications éventuelles à apporter à l'infrastructure	\$					
Début de l'achat d'équipements : serveurs, appareils de télécommunication, dispositifs de sauvegarde temporaire et de stockage à long terme				\$		
Début de l'achat de logiciels : courriel, sécurité, gestion des documents, classification des documents					\$	

De six à neuf mois

Tâches	Conception et élaboration	Temps des formateurs et des participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Modification et mise à l'essai de l'infrastructure (gestion des courriels, sécurité, récupération en cas de sinistre)	\$		\$	\$	\$	
Mise à l'essai et finalisation des procédures	\$					
Préparation et mise à l'essai de plans de surveillance de la conformité						\$
Préparation de documents de sensibilisation	\$	\$				
Élaboration de documents pédagogiques relativement à la politique, aux procédures et à l'infrastructure en gestion des courriels		\$				



De neuf à douze mois

Tâches	Conception et élaboration	Formateurs et participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Démarrage d'un programme de sensibilisation à la gestion des courriels, afin de préparer les utilisateurs à la mise en œuvre des Lignes directrices	\$	\$				
Début des formations destinées à préparer les employés, contractuels et autres utilisateurs à la mise en œuvre des Lignes directrices	\$	\$	\$	\$	\$	

Après douze mois

Tâches	Conception et élaboration	Formateurs et participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Fin de la mise en œuvre des Lignes directrices	\$					
Début de la surveillance de la conformité						\$
Identification et réparation des bogues initiaux	\$					



Autres coûts potentiels

Tâches	Conception et élaboration	Formateurs et participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Consultants externes	\$	\$				\$
Adaptation ou configuration des logiciels	\$					
Migration des données	\$					

Coûts totaux

Tâches	Conception et élaboration	Formateurs et participants aux formations	Espaces physiques	Équipements	Logiciels	Surveillance de la conformité
Coûts totaux	\$	\$	\$	\$	\$	\$



ANNEXE C. LOIS, RÈGLEMENTS, POLITIQUES ET ENTENTES QUI NÉCESSITENT L'APPLICATION DES LIGNES DIRECTRICES POUR LA GESTION DES COURRIELS

Lois nécessitant l'application des Lignes directrices

Les lois listées ci-dessous ne prescrivent pas expressément une norme ou des lignes directrices particulières en matière de gestion des courriels; elles établissent toutefois certaines responsabilités et obligations légales relatives à la divulgation (et à la non-divulgation), et à l'élimination de l'information, incluant l'information électronique. Cette dernière comprend ou peut être interprétée comme comprenant les courriels, leurs métadonnées et pièces jointes.

Les courriels peuvent être exigés lors d'une action en justice, d'un audit ou d'une demande d'accès à l'information.

Les présentes Lignes directrices pour la gestion des courriels sont conçues pour faciliter le respect des responsabilités et obligations décrites dans les lois listées ci-dessous.

Les institutions du gouvernement canadien ne sont pas tenues de documenter leur processus décisionnel ou leurs actions, à l'exception des transactions financières. Cependant, si de telles informations sont recueillies par une institution, celle-ci doit en assurer la conservation durant une période de temps appropriée.

Accès à l'information, Loi sur l'

La Loi offre l'accès aux documents de l'administration fédérale en consacrant le principe du droit du public à leur communication, les exceptions indispensables à ce droit étant précises et limitées et les décisions quant à la communication étant susceptibles de recours indépendants du pouvoir exécutif.

(Source : <http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03-fra.asp>)



Bibliothèque et les Archives du Canada, Loi sur la

Cette loi définit la mission et les attributs de Bibliothèque et Archives Canada, ainsi que les exigences légales concernant l'élimination et l'aliénation des documents du gouvernement et des ministères.

(Source : <http://laws.justice.gc.ca/fr/L-7.7/>)

Charte canadienne des droits et libertés

La Constitution canadienne comprend un ensemble de documents qui établissent les pouvoirs exécutifs, législatifs et judiciaires du gouvernement, attribuent les pouvoirs du gouvernement fédéral et définissent les droits des citoyens. La Charte canadienne des droits et libertés constitue l'annexe B de la Loi constitutionnelle de 1982. Elle garantit les libertés et les droits fondamentaux de chaque individu qui ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse être démontrée dans le cadre d'une société libre et démocratique.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Crédits, Lois de

Ces lois établissent les programmes, les services et les activités du gouvernement et permettent d'allouer le financement annuel pour leur développement et leur exploitation. L'information ministérielle sur la planification fournit les éléments de base permettant de mesurer les résultats atteints.

L'information est présentée comme un article de dépense en fonction duquel les prévisions budgétaires sont réparties. L'information renferme trois principales catégories de dépenses : les services de publicité; les services d'édition, d'impression et d'exposition; les services de relations et d'affaires publiques.

Les lois déterminent et financent les secteurs d'activités des ministères, y compris le secteur de la technologie de l'information et de la gestion de l'information du Conseil du Trésor, en vue d'assurer l'orientation et le leadership stratégiques pour tirer parti de la technologie de l'information et de la gestion de l'information afin d'améliorer l'accès du public aux services gouvernementaux et d'atteindre les objectifs de renouvellement de la fonction publique.

(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)



Droit d'auteur, Loi sur le

La Loi vise à établir et à protéger la possession du droit d'auteur et les droits correspondants pour produire ou reproduire des oeuvres ou toutes parties substantielles de celles-ci sous forme matérielle, pour les exécuter ou pour les publier. La Loi renferme des définitions pour la propriété intellectuelle et établit des règles relatives à la possession du droit d'auteur. La Loi établit les actions qui représentent des violations, indique les recours auxquels l'auteur a droit en cas de violation, établit le Bureau du droit d'auteur chargé de traiter les demandes de droit d'auteur et de maintenir un registre des droits d'auteur et établit la Commission du droit d'auteur chargée d'appliquer la Loi, de rendre des décisions et d'attester les redevances. Nota : En vertu de la Politique sur les services communs, Travaux publics et Services gouvernementaux Canada est responsable de l'administration des droits d'auteur de la Couronne.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Emploi dans la fonction publique, Loi sur l'

La Loi établit la Commission de la fonction publique et détermine les principes et les conditions régissant le recrutement et la nomination du personnel et d'autres aspects de l'emploi dans la fonction publique tels que les recours, les mises en disponibilité, les nominations prioritaires et les activités politiques.

(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_fra.asp)

Gestion des finances publiques, Loi sur la

La Loi établit le Conseil du Trésor et le ministère des Finances et prévoit l'administration des ressources financières et humaines du gouvernement du Canada, la création et la tenue des comptes du Canada et le contrôle des sociétés d'État. Cette Loi s'applique tout particulièrement à la gestion de l'information pour ce qui est de la délégation des autorisations administratives et des dispositions exigeant la tenue de transactions et de documents fédéraux appropriés. L'accès à une information de qualité et ponctuelle est essentiel à la prise de décisions, à l'exécution des activités, aux besoins de preuve, à des fins historiques, pour assurer l'accès au public et pour surveiller continuellement et améliorer les programmes et les services. Note : D'autres lois telles que la Loi sur l'emploi dans la fonction publique, la Loi sur les relations de travail dans la



fonction publique, la Loi sur la pension de retraite et le Code canadien du travail traitent tout particulièrement des ressources humaines

(Source : <http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03-fra.asp>)

Langues officielles, Loi sur les

La Loi établit que le français et l'anglais sont les langues officielles du Canada et établit des dispositions permettant de s'assurer qu'ils ont un statut et des droits et privilèges égaux quant à leur usage dans toutes les institutions fédérales.

(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_fra.asp)

Preuve au Canada, Loi sur la

Décrit les rôles et les procédures à l'égard des témoins et des preuves dans le cadre de procédures pénales et civiles ainsi que toutes les autres matières de compétence fédérale. La Loi détermine la nature et les caractéristiques de l'information qui est admissible comme preuve et celle qui ne l'est pas. (Voir aussi la Loi sur la protection des renseignements personnels et les documents électroniques).

Identifie les catégories de preuves documentaires qui peuvent être utilisées dans le cadre d'une procédure judiciaire. Prévoit des dispositions à l'égard de l'information (version originale ou copie) qui peut être acceptée comme document officiel dans le cadre d'une procédure judiciaire et décrit les conditions d'admissibilité de la preuve. Établit les règles d'admissibilité en preuve des documents électroniques, et l'utilisation des normes, des procédures, de l'usage ou des pratiques concernant la manière dont les documents électroniques sont enregistrés ou mis en mémoire.

Prévoit des dispositions en cas d'opposition à la divulgation de renseignements devant un tribunal, un organisme ou une personne ayant le pouvoir de contraindre à la production de renseignements, en attestant verbalement ou par écrit devant eux que ces renseignements ne devraient pas être divulgués pour des raisons d'intérêt public déterminées.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)



Protection civile, Loi sur la

La Loi sur la protection civile prévoit les mesures de protection civile nécessaires pour préparer le pays à faire face aux situations de crise de toute nature en définissant les responsabilités en ce qui a trait à l'élaboration et à la mise en œuvre de plans d'intervention civils, y compris la conservation des documents essentiels et la planification pour la reprise des activités.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Protection de l'information, Loi sur la

Cette loi définit les infractions reliées à la divulgation de l'information dans un dessein nuisible à la sécurité ou aux intérêts du Canada.

(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_fra.asp)

Protection des renseignements personnels et les documents électroniques, Loi sur la

Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la Loi sur la preuve au Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois. Certains organismes régis par le gouvernement fédéral et non assujettis à la Loi sur la protection des renseignements personnels tels que des éléments de Postes Canada sont régis par la présente Loi. (Voir aussi la Loi sur la Preuve au Canada)

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_fra.asp)



Protection des renseignements personnels et règlements afférents, Loi sur la

Assurer la protection des renseignements personnels relevant des institutions fédérales et assurer le droit d'accès des individus aux renseignements personnels qui les concernent. Les exigences en matière d'information sont résumées ci-après et présentées plus en détail à l'annexe B qui établit une mise en correspondance avec le Cadre de gestion de l'information.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_f.asp)

Responsabilité civile de l'État et le contentieux administratif, Loi sur la

La Loi détermine la responsabilité du gouvernement, et les règles et procédures en cas de poursuites judiciaires par l'État ou contre celui-ci. La responsabilité en matière d'information est présentée tout particulièrement dans le contexte de l'atteinte à la vie privée.

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Service canadien de renseignement de sécurité, Loi sur le

Établit le Service canadien du renseignement de sécurité pour mener des enquêtes et conseiller le gouvernement au sujet d'activités qui peuvent constituer une menace pour la sécurité du Canada. La Loi renferme des dispositions spéciales pour l'accès à l'information dans l'intérêt de la sécurité nationale.

(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Statistique, Loi sur la

La Loi prévoit la collecte, la compilation, l'analyse, le dépouillement et la publication de renseignements statistiques sur les activités commerciales, industrielles, financières, sociales, économiques et générales de la population et sur l'état de celle-ci.



(Source: http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg04_f.asp)

Vérificateur général, Loi sur le

Établit le rôle du vérificateur général consistant à mener des vérifications au sujet des ministères et des organismes fédéraux, des sociétés d'État et des comptes du Canada et à présenter les résultats à la Chambre des communes. Le vérificateur général assure une évaluation indépendante des activités du gouvernement qui compte grandement sur la disponibilité d'une information de qualité et il formule des observations et des recommandations fondées, du moins en partie, sur l'évaluation de l'information disponible.

Le vérificateur général a le droit d'avoir accès à l'information, aux rapports et aux explications des ministères et des sociétés d'État dont il a besoin pour assumer ses responsabilités et il indiquera dans son rapport annuel si l'information nécessaire lui a été fournie. (13, 14, 7)

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg03_fra.asp)

Politiques et directives fédérales nécessitant les Lignes directrices pour la gestion des courriels

Le Cadre de la gestion de l'information (CGI) au sein du gouvernement du Canada procure une orientation stratégique et pratique. Il indique les motifs justifiant l'intégration de la gestion de l'information et les moyens d'y parvenir, par un vaste éventail d'activités du GdC pour améliorer les opérations, la conformité aux lois et aux politiques, l'accès aux services par les citoyens et la reddition de comptes. L'orientation établie par le CGI peut servir « telle quelle » ou être modifiée en fonction des besoins particuliers de l'organisation.

(Source : <http://www.tbs-sct.gc.ca/fmi-cgi/index-fra.asp>)

La Politique sur la gestion de l'information exige des institutions gouvernementales qu'elles gèrent leurs documents tout au long de leur cycle de vie.

La Directive sur les rôles et responsabilités en matière de gestion de l'information identifie les rôles et responsabilités de tous les employés du gouvernement en ce qui concerne la gestion de l'information.



La Politique sur la Sécurité identifie les exigences requises afin de garantir que toute information du gouvernement fédéral, classifiée ou désignée, soit correctement sauvegardée.

(Source : http://www.tbs-sct.gc.ca/cio-dpi/pols_fra.asp)

Plusieurs autres politiques nécessitent le recours aux présentes Lignes directrices, ou imposent elles-mêmes des normes ou des lignes directrices en matière de gestion des courriels.

- Accès à l'information, Politique sur l'
- Apprentissage, de formation et de perfectionnement, Politique en matière d'
- Autorisation et l'authentification électroniques, Politique sur l'
- Communication, Politique de
- Évaluation, Politique d'
- Évaluation des facteurs relatifs à la vie privée, Politique d'
- Gestion de l'information, Politique sur la
- Gestion de l'infrastructure à clé publique, Politique de
- Gestion des projets, Politique sur la
- Gestion des risques, Politique sur la
- Gestion des technologies de l'information, Politique sur la
- Protection des renseignements personnels, Politique sur la
- Sécurité, Politique sur la
- Services communs, Politique sur les
- Utilisation des réseaux électroniques, Politique d'



ANNEXE D. TABLEAU DES NORMES TECHNIQUES ET PROCÉDURALES

Le tableau ci-dessous dresse la liste des lignes directrices proposées dans le présent document, qu'elles soient de nature technique ou procédurale, ou un mélange des deux. Le tableau précise si les procédures sont surtout manuelles ou si elles peuvent être automatisées, au moins dans une certaine mesure.

Spécifications techniques	Procédure possiblement automatisée	Procédure manuelle	Normes/ Ligne directrices
			1. Les institutions doivent se doter d'un plan pour gérer les courriels
	✓	✓	1.1. Gérer les programmes et les systèmes de courriel de manière intégrée
		✓	1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels
		✓	1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels
		✓	1.4. Vérifier que les Lignes directrices pour la gestion des courriels ainsi que les politiques et procédures associées ont bien été distribuées, lues et comprises
		✓	1.5. Conserver des dossiers sur les activités de formation et sur la participation
			2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles
✓	✓	✓	2.1. Créer, expédier et stocker les courriels de manière structurée
	✓	✓	2.2. Recevoir et stocker les courriels de manière structurée
		✓	2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière
			2.4. Garder un seul exemplaire de chaque courriel
✓	✓	✓	2.5. Gérer et conserver les pièces jointes aux courriels
✓		✓	2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada



Spécifications techniques	Procédure possiblement automatisée	Procédure manuelle	Normes/ Ligne directrices
		✓	2.7. Utiliser avec modération les listes de diffusion institutionnelles
✓	✓	✓	2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource
			2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu
			2.10. Utiliser un avis d'opinion personnelle, s'il y a lieu
		✓	2.11. Éviter d'utiliser la fonction « Répondre à tous »
			3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles
✓	✓	✓	3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels
	✓	✓	3.2. Déterminer où classer la « copie officielle »
✓	✓		3.3. Conserver les métadonnées associées aux courriels
	✓	✓	3.4. Classifier et classer les courriels systématiquement et fréquemment
✓	✓	✓	3.5. Gérer le stockage en ligne temporaire des courriels
		✓	3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels
		✓	3.7. Limiter le contenu des courriels à un seul sujet
		✓	3.8. Décrire l'objet d'un courriel en termes clairs et significatifs
✓	✓		3.9. Prévoir un système d'indexation des courriels
			3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (<i>threading</i>)
			4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels
		✓	4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en



Spécifications techniques	Procédure possiblement automatisée	Procédure manuelle	Normes/ Ligne directrices
			vigueur
✓			4.2. Utiliser les journaux d'exploitation pour constituer une piste de vérification et veiller au respect des règles
✓			4.3. Afficher les noms dans les en-têtes et les adresses de courriel
✓		✓	4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique
			4.5. Surveiller la performance des activités de découverte et de disposition des courriels
			5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés
			5.1 Éviter de procéder à des purges indiscriminées dans les systèmes de courriel
✓		✓	5.2. Gérer les courriels de façon à permettre l'accès aux personnes autorisées
			5.3. Enlever le chiffrement avant de quitter une institution
			5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada
✓			5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel
✓		✓	5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets
✓			5.7. Protéger les systèmes contre les pertes ou les dommages
			5.8. Employer le bon niveau de classification de sécurité
✓	✓	✓	5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun
✓			5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel
✓			5.11. Utiliser des mesures de protection et d'authentification des messages
✓			5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre



Spécifications techniques	Procédure possiblement automatisée	Procédure manuelle	Normes/ Ligne directrices
✓		✓	5.13. Utiliser la signature numérique s'il y a lieu
✓			5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada
		✓	5.15. Ne pas employer de signature numérisée pour signer un courriel
✓		✓	5.16. Utiliser le chiffrement s'il y a lieu
✓	✓	✓	5.17. Employer le stockage de proximité pour la conservation à long terme des courriels
			5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore
✓			5.19. Protéger les courriels en protégeant les supports de conservation
✓			5.20. Protéger les courriels de l'obsolescence
✓		✓	5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel
		✓	5.22. Conserver en permanence la documentation du système de courriel
✓	✓	✓	5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes
✓		✓	5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document
			6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes
		✓	6.1. Obtenir une autorisation de disposition des courriels
✓	✓	✓	6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun
✓			6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP
IPRP			7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin



Spécifications techniques	Procédure possiblement automatisée	Procédure manuelle	Normes/ Ligne directrices
			7.1. Évaluer l'efficacité de la gestion des courriels
			8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels
		✓	8.1. Responsabilités des utilisateurs
		✓	8.2. Responsabilités des administrateurs de réseaux ou de systèmes
		✓	8.3. Responsabilités des spécialistes en gestion de l'information
		✓	8.4. Responsabilités des gestionnaires des opérations
		✓	8.5. Responsabilités des dirigeants