



SOCIÉTÉ DE
TRANSPORT
DU SAGUENAY

POLITIQUE SUR LA RÉTENTION DES DONNÉES

Dernière mise à jour : 23 septembre 2024.

PERSONNES-RESSOURCES	
Responsables :	Titres :
Principal : Responsable de la protection des renseignements personnels.	Secrétaire générale et conseillère juridique.
En soutien : Département des technologies de l'information;	Directeur de la planification réseau, projets et électrification et les membres de son équipe sous sa supervision.
APPROBATION	
Approuvé par :	Date :
Responsable de la protection des renseignements personnels;	Le 23 septembre 2024.
Conseil d'administration de la Société de transport du Saguenay.	

Section 1. CHAMP D'APPLICATION

- 1.1 La présente politique s'applique à tous les documents générés, reçus ou conservés par la Société de transport du Saguenay (la « **STS** »).
- 1.2 La présente politique régit tous les documents sous la garde de la STS, incluant notamment les dossiers, correspondances, notes de service, courriels, messages instantanés, contrats, rapports, fichiers de travail, calendriers et autres. Cette catégorie englobe aussi bien les formats papier que les formats électroniques, comme les courriels, les documents de traitement de texte, les bases de données et toute information enregistrée sur un ordinateur (les « **Documents de la STS** »). Elle s'étend à tout ce qui peut contenir des renseignements personnels sur les employés et les autres intervenants de la STS, aux termes des lois applicables sur la protection de la vie privée.
- 1.3 Les Documents de la STS sont la propriété de cette dernière, et non la propriété personnelle des employés. Le texte ci-dessous présente la politique de la STS concernant la conservation, la protection et la destruction de ces documents.

Section 2. BUT

2.1 La présente politique a pour but :

- (a) d'assurer que la STS, ses administrateurs, ses dirigeants et ses employés conservent et protègent les Documents de la STS conformément aux lois et règlements applicables;
- (b) d'assurer que la STS adopte les procédures nécessaires pour protéger les renseignements personnels en sa possession et se conformer aux lois applicables sur la protection de la vie privée;
- (c) de protéger la STS, ses administrateurs, ses dirigeants et ses employés contre les risques associés à la destruction accidentelle ou inopportune des Documents de la STS devant être conservés à des fins juridiques;
- (d) de protéger les intérêts commerciaux de la STS.

2.2 Le non-respect de la présente politique pourrait exposer la STS, ses administrateurs, ses dirigeants et ses employés à des amendes, des sanctions et des dommages non négligeables. Le non-respect pourrait ainsi être puni par des mesures disciplinaires progressives pouvant aller jusqu'à la suspension et au congédiement.

Section 3. RÔLES ET RESPONSABILITÉS

3.1 Responsable de la protection des renseignements personnels

- (a) Le responsable de la protection des renseignements personnels est responsable de la mise à jour et l'approbation de la présente politique.

3.2 Gestionnaire

- (a) Le service de la STS responsable du respect de la présente politique relativement à un document est celui l'ayant généré.
- (b) Le gestionnaire du service responsable ou son délégué tient l'équipe sous sa responsabilité informée de la présente politique et assure la conservation, la protection et la destruction des documents en conséquence.
- (c) Le gestionnaire du service responsable ou son délégué définit la marche à suivre pour la rétention et la destruction des documents dont il est responsable et voit à ce que toutes les précautions raisonnables soient prises pour assurer la sécurité et la confidentialité des renseignements personnels et confidentiels à détruire (y compris durant leur conservation, entreposage, transport, manutention et destruction). Il peut consulter l'équipe technique et la direction afin d'obtenir de l'assistance dans la mise en place de ce processus.

3.3 Employés

- (a) La STS compte sur tous ses employés pour respecter la présente politique et les calendriers de conservation approuvés par la Direction, en application de celle-ci.
- (b) Tous les employés doivent : (i) créer, recueillir et verser leurs documents dans un système de stockage fiable et sécuritaires, pour que ces documents y soient conservés, protégés

et détruits (en temps voulu) conformément aux présentes; et (ii) conserver tous les documents associés à un litige, conformément à l'Section 4 (Documents conservés en vue d'un litige) ci-dessous.

Section 4. DOCUMENTS CONSERVÉS EN VUE D'UN LITIGE

- 4.1 Nonobstant les autres dispositions de la présente politique, la règle suivante s'applique à tous les documents : **Si vous croyez ou si un autre intervenant de la STS vous informe qu'un document est ou pourrait être utile à un litige réel ou potentiel (par exemple, un différend pouvant mener à un litige, même si ce n'a pas encore été le cas), vous devez immédiatement en informer la Direction de la STS et prendre les mesures nécessaires pour conserver ces documents, qu'ils soient en format papier ou électronique, en attendant que la Direction détermine s'il faut les conserver.**
- 4.2 La Direction prendra les mesures nécessaires pour vérifier si la STS a l'obligation de préserver ces documents. Le cas échéant, ils en informeront les personnes concernées et préciseront les documents ou types de documents visés.
- 4.3 **Lorsque des documents sont conservés en vue d'un litige, toutes les règles habituelles concernant la destruction de ces documents sont immédiatement suspendues.** Cette suspension se poursuit jusqu'à que la Direction avise de la fin de cette période par écrit et autorise la reprise du processus normal de destruction.
- 4.4 Il est absolument interdit d'ouvrir ou de modifier un document électronique pendant sa conservation en vue d'un litige. Si vous devez consulter un tel document électronique dans l'exercice de vos fonctions habituelles pour la STS, demandez l'aide de la Direction.
- 4.5 Aux fins des présentes, le terme « *litige* » comprend les poursuites civiles entamées par ou contre la STS, ainsi que les enquêtes réglementaires, les poursuites en matière réglementaire, criminelle ou fiscale, et les poursuites civiles contre un dirigeant, un administrateur ou un employé de la STS qui concernent la STS. On compte aussi les cas d'arbitrage et autres processus de règlement des différends.
- 4.6 Si vous êtes mis au courant d'une situation qui pourrait mener à un litige, communiquez immédiatement avec la Direction de la STS.

Section 5. ARCHIVAGE

- 5.1 Les copies papier des Documents de la STS sont normalement conservées par le service qui les a créées ou reçues, à moins d'approbation contraire du gestionnaire compétent.
- 5.2 Dans la mesure du possible, ces documents doivent être classés par type (p. ex., document comptable, base de données, audits, dossiers des ressources humaines) et s'accompagner de précisions sur le délai et le format de conservation (p. ex., papier, magnétique, optique).
- 5.3 Des mesures adéquates doivent être prises en tout temps pour protéger les Documents de la STS.
- 5.4 En aucun cas les Documents de la STS ne doivent être conservés dans une résidence personnelle.

Section 6. CALENDRIER DE RÉTENTION

- 6.1** Les délais de rétention sont indiqués à l'annexe A (*Calendrier de rétention*) ci-dessous. Les Documents de la STS contenant des renseignements personnels sur les employés ou d'autres personnes sont aussi soumis notamment aux normes de rétention et de destruction établies par les lois sur la protection des renseignements personnels applicables, conformément à l'annexe B (*Renseignements personnels*).
- 6.2** Outre les normes de conservation législatives décrites aux annexes A et B ci-dessous, **la STS a pour politique de conserver indéfiniment** : les contrats, licences, baux, documents hypothécaires, servitudes, permis, titres et documents relatifs à un droit, un titre ou un intérêt dans un bien de la STS (y compris les droits de propriété intellectuelle). Ces documents ne doivent pas être détruits sans l'approbation du gestionnaire concerné et de la Direction.
- 6.3** Pour fixer les périodes de rétention, en plus des obligations définies aux présentes (notamment aux paragraphes 6.1 et 6.2), la Direction doit tenir compte :
- (a) de l'utilité du document dans le cadre des affaires et des activités de la STS;
 - (b) de la valeur historique éventuelle du document;
 - (c) des obligations contractuelles de la STS, notamment quant à la rétention ou la destruction des documents (et aux renseignements confidentiels d'un tiers contenus dans une convention de non-divulgation ou de confidentialité);
 - (d) de l'éventualité d'un litige dans lequel le document serait utile ou d'une enquête réglementaire, d'audit ou d'une demande d'accès à l'information;
 - (e) des délais de prescription prévus par le droit applicable;
 - (f) des coûts associés à l'archivage et à l'entretien des documents, par exemple les coûts potentiels de la production de documents sous la garde de la STS en cas de litige, d'enquête réglementaire ou d'autres processus de recherche imprévus.
- 6.4** Le calendrier de rétention doit tenir compte du fait que chaque période est enclenchée par un événement donné. Cet événement peut être la date de création du document, sa date de fin d'utilisation courante par la STS, etc. Pour calculer la période de rétention qui s'applique à une catégorie de documents, il faut d'abord déterminer la date de début de la rétention. On évitera ainsi de détruire un document prématurément.
- 6.5** Quand plusieurs périodes de conservation s'appliquent à un même document aux termes des présentes, c'est la plus longue qui s'applique.

Section 7. DOCUMENTS ÉLECTRONIQUES

7.1 Périodes de rétention

Aux fins de la politique, les « documents électroniques » englobent tous ceux qui ne sont pas en format papier. Les périodes de rétention énoncées aux présentes s'appliquent aux documents papier comme électroniques.

7.2 Courriels

Les courriels sont des documents électroniques importants pour la STS. Par exemple, ils peuvent notamment:

- (a) prouver la conclusion d'un contrat ou la délivrance d'un avis;
- (b) contenir des renseignements personnels devant être conservés pendant un certain temps selon les lois sur la protection des renseignements personnels applicables;
- (c) contenir des renseignements utiles au calcul de l'impôt, qui doivent être conservés selon différentes lois fiscales;
- (d) contenir des renseignements utiles à de futures négociations avec un tiers;
- (e) constituer la preuve d'un comportement fautif;
- (f) prouver que les exigences de déclaration obligatoire aux organismes de réglementation ont été respectées.

Par conséquent, les courriels doivent être traités comme tout autre document aux fins des présentes.

7.3 Documents en format papier seulement

- (a) Outre les obligations imposées par les lois applicables concernant le maintien d'un document dans son format original, les types de documents papier suivants doivent rester en format papier, qu'ils aient été numérisés ou non : (i) les documents conservés en vue d'un litige; (ii) les procurations relatives aux biens ou aux soins à la personne; et (vii) les originaux signés d'affidavits et d'autres documents juridiques.
- (b) Pour savoir si un type de document doit être conservé en format papier, consultez la Direction de la STS avant de détruire la version papier.

7.4 Conservation des documents électroniques

- (a) Des mesures adéquates doivent être prises en tout temps pour protéger l'exactitude, la sécurité et l'intégrité des documents électroniques traités et tenus par la STS.
- (b) Tous les documents électroniques doivent être conservés dans le format dans lequel ils ont été créés, envoyés ou reçus, ou dans un format qui n'altère pas l'information qui s'y trouve. L'information du document électronique doit être lisible et consultable pour les personnes qui ont le droit d'accéder au document ou de participer à sa production pendant la période de rétention applicable. Si le document électronique a été envoyé ou reçu, l'information sur son origine et sa destination doit aussi être conservée, tout comme la date et l'heure de l'envoi ou de la réception. Il faut aussi conserver les métadonnées associées à un document électronique.
- (c) Dans certains cas, la loi ou le règlement applicable impose des exigences supplémentaires pour la rétention de documents électroniques, notamment quant à l'endroit où ils sont enregistrés. Par exemple, les documents électroniques dont la rétention est obligatoire aux termes de la *Loi de l'impôt sur le revenu* du Canada doivent être enregistrés conformément aux directives régissant le stockage à long terme de ce type de documents (voir la circulaire d'information 78-10R5 de l'Agence du revenu du

Canada). Consultez les lois et les règlements applicables pour voir s'il y a des exigences de conservation sous forme électronique ou papier.

- (d) Les documents électroniques doivent être enregistrés et conservés dans un système de gestion de l'information approprié.

Section 8. DESTRUCTION DE DOCUMENTS

- 8.1** Sous réserve du paragraphe 8.5, les documents de la STS doivent généralement être détruits à l'expiration de la période applicable du calendrier de rétention.
- 8.2** Sous réserve du paragraphe 8.5, il incombe au gestionnaire ou à son délégué d'établir le processus de destruction des Documents de la STS pour les activités ou les fonctions de soutien qu'il chapeaute. Ce processus doit au minimum respecter les modalités de la présente politique. L'OC (*Destruction de documents*) énonce les exigences minimales de destruction sécuritaire.
- 8.3** Un document ne doit jamais être partiellement détruit ou autrement modifié si cela a pour effet de créer un ensemble de faits trompeurs, que ce soit par omission ou autrement.
- 8.4** Les Documents de la STS pour lesquels la période de rétention est expirée doivent, si possible, être détruits ou retirés de tout endroit physique ou support électronique servant à leur conservation, y compris les courriels, les classeurs, les aires d'entreposage inactives, les supports magnétiques ou optiques et les sauvegardes.
- 8.5** Les documents de la STS conservés en vue d'un litige ne doivent pas être détruits tant que l'affaire n'est pas terminée et tant que la Direction n'a pas approuvé par écrit la reprise du processus normal de destruction. Ces documents doivent être isolés ou porter une mention claire pour éviter qu'ils soient accidentellement détruits au cours d'un processus normal.
- 8.6** Les renseignements personnels des employés de la STS ou d'autres personnes qui ne sont plus requis aux fins auxquelles ils ont été recueillis et qui ne sont pas soumis à une période de rétention aux termes des lois applicables ni conservés en vue d'un litige doivent être détruits.

Les renseignements personnels et autres renseignements confidentiels doivent être détruits d'une manière qui préserve leur confidentialité et les rend impossibles à reconstituer ou récupérer.

ANNEXE A Calendrier de rétention

Certaines catégories de documents sont énumérées ici à des fins d'accessibilité. [Une liste détaillée des types de documents opérationnels et des périodes de rétention applicables pour chacun sera joint (intitulé « Calendrier de rétention ») en Annexe A-2. Les règles énoncées au Calendrier de rétention s'applique que le document soit en format papier ou électronique. Veuillez-vous y référer pour déterminer la période de rétention appropriée. S'il y a incohérence entre la présente politique, le Calendrier de rétention et les lois applicables, la période de rétention la plus longue prévaut].

- Dossiers fiscaux. Les dossiers d'impôt comprennent notamment les documents concernant les informations relatives à la paie, les preuves de retenues, les coûts opérationnels et les procédures comptables ainsi que d'autres documents relatifs aux revenus et aux dépenses de la STS. Ils doivent être conservés pendant au moins les **sept (7) années suivant l'année d'imposition visée**.
- Dossiers d'emploi/du personnel. La STS conserve les dossiers du personnel renfermant notamment les évaluations de performance, les plaintes formulées et les mesures prises à l'égard de l'employé pendant une période de **trois (3) ans après la cessation d'emploi**.
- Documents du conseil d'administration. Les procès-verbaux et les résolutions conseil d'administration doivent être conservés **à perpétuité** dans le registre des procès-verbaux ou les dossiers pertinents de la STS. Une copie de tous les documents présentés lors des réunions du conseil d'administration doit être conservée à perpétuité en format électronique.
- Communiqués de presse/documents d'information publics. La STS doit conserver des **copies permanentes** de tous les communiqués de presse et de tous les documents publics si jamais elle doit vérifier l'exactitude d'un document qu'un membre du public produit contre elle.
- Documents ayant une valeur juridique ou constatant un fait juridique. Les documents ayant une valeur juridique ou constatant un fait juridique doivent généralement être conservés durant une période minimale de **dix (10) ans**, mais il est indiqué de consulter un conseiller juridique pour déterminer la période appropriée pour certains documents particuliers. S'il y a un risque de litige, il est préférable de conserver les documents durant la plus longue période permise.
- Contrats. Des copies définitives et signées de tous les contrats conclus par la STS doivent être conservées pendant **au moins sept (7) ans après leur échéance**, et plus longtemps s'il s'agit de contrats déposés publiquement. Les factures de vente, les baux, les licences et les autres documents juridiques devraient également être conservés **pendant au moins les sept (7) années suivant leur échéance**. S'il y a un risque de litige, il est préférable de conserver les documents durant la plus longue période permise.
- Courriels. La période de conservation dépend du sujet du courriel, comme il est mentionné ailleurs dans la présente politique.

ANNEXE B

Renseignements personnels

1. *En quoi consistent les renseignements personnels?*

- (a) En général, ce sont des renseignements qui permettent *d'identifier une personne*. Il peut s'agir de renseignements sur une *personne identifiée* (on connaît son identité ou son nom) ou *que l'on est capable d'identifier* (on ne connaît pas son identité ou son nom, mais on est en mesure de l'identifier au moyen des renseignements fournis ou disponibles).
- (b) Sont des exemples de renseignements personnels les antécédents professionnels, les renseignements sur la santé, l'information financière et les renseignements sur la famille *d'une personne*. Le nom et les coordonnées personnelles, y compris l'adresse courriel, d'une personne sont également des renseignements personnels.
- (c) Le nom, le titre ainsi que l'adresse, le courriel et le numéro de téléphone professionnels d'un employé (les « **Coordonnées professionnelles** ») recueillis, utilisés ou communiqués par la STS uniquement pour entrer en contact avec lui dans le cadre de son emploi, de son entreprise ou de sa profession ne sont pas assujettis aux mêmes restrictions que les renseignements personnels dont il est question ci-dessous.
- (d) Les renseignements sur une autre société ou organisation ne constituent pas des renseignements personnels. Cependant, les renseignements recueillis, utilisés ou communiqués par la STS au sujet des administrateurs, des dirigeants, des clients et des employés (autres que les Coordonnées professionnelles) doivent être considérés comme des renseignements personnels. Par exemple, si XYZ Inc. offre un service à la STS, le nom et le numéro de téléphone professionnel du représentant commercial de XYZ Inc. avec qui vous avez traité ne sont pas considérés comme des renseignements personnels s'ils sont utilisés uniquement dans le cadre de ce service. Par contre, les renseignements concernant sa vie personnelle ou permettant d'identifier des administrateurs, des dirigeants ou des clients de XYZ Inc. (autres que des Coordonnées professionnelles) sont des renseignements personnels.
- (e) Si vous n'êtes pas en mesure de déterminer si des renseignements sont de nature personnelle ou non, consultez notre personne responsable de la protection des renseignements personnels.

2. *Rétention des renseignements personnels*

- (a) Les pratiques de rétention de la STS doivent respecter les lois fédérales et provinciales sur la protection des renseignements personnels, qui renferment leur propre période de rétention minimale et maximale pour les renseignements personnels.
- (b) De façon générale, les renseignements personnels doivent être conservés aussi longtemps que nécessaire pour répondre aux besoins pour lesquels ils ont été recueillis, à moins qu'une période de rétention plus longue ne soit exigée ou permise par la loi. Par exemple, aux termes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels qui ne sont plus nécessaires pour répondre aux besoins pour lesquels ils ont été recueillis doivent être détruits ou effacés, à moins que leur rétention ne soit exigée par la loi. Veuillez noter que seuls les renseignements personnels, et non les dossiers contenant ces renseignements, doivent être éliminés.
- (c) La législation sur la protection des renseignements personnels comprend des exigences de rétention minimales pour certains types de renseignements personnels. Dans le cas où une personne a demandé l'accès à ses renseignements personnels ou la modification de ceux-ci, **les**

renseignements en question doivent être conservés suffisamment longtemps pour que la personne concernée épuise tous les recours prévus par les lois applicables en ce qui a trait à une telle demande. De plus, si des renseignements personnels sont utilisés pour prendre une décision qui concerne directement une personne, la législation sur la protection des renseignements personnels exige que ces renseignements soient conservés durant une période minimale d'une (1) année.

- (d) Lorsque la STS cesse d'utiliser des documents renfermant des renseignements personnels aux fins pour lesquelles ils ont été recueillis, elle doit déterminer si les dossiers en question sont visés par une exigence légale de rétention ou un avis de conservation pour litige. Si tel est le cas, les documents doivent être conservés pendant la période applicable.
- (e) Toutes les périodes de rétention pour des renseignements personnels doivent être fixées par le gestionnaire (ou son délégué) en consultation avec la personne responsable de la protection des renseignements personnels de la STS.
- (f) Si vous avez connaissance d'une atteinte réelle ou potentielle à la vie privée, d'une communication non autorisée ou de la perte de renseignements personnels, vous devez en aviser immédiatement la personne responsable de la protection des renseignements personnels.

ANNEXE C

Destruction de documents

Cette annexe contient une liste de vérification pour la destruction des Documents de la STS dans le cadre de ses activités normales. Elle assure la destruction sécuritaire des documents contenant des renseignements personnels, selon les exigences des lois sur la protection des renseignements personnels applicables. Un gestionnaire peut autoriser la destruction des documents au moyen d'un autre procédé, pourvu que le procédé en question garantisse la destruction sécuritaire des documents ainsi que la sécurité et la confidentialité des renseignements personnels ou autres renseignements qu'ils renferment, et que le procédé en question et les documents détruits soient adéquatement consignés. La personne responsable de la protection des renseignements personnels doit être consultée dans le cadre de ce processus.

1. **Indiquer quels sont les documents à détruire** : Une liste des documents que l'on envisage de détruire doit être fournie au gestionnaire concerné (ou à son délégué). Aucune démarche ne doit être entreprise avant que le gestionnaire (ou son délégué) n'ait donné son approbation pour la destruction.

2. **Sélectionner et recruter un fournisseur de services externe avec prudence** : Si la destruction des Documents de la STS est confiée à un fournisseur de services externe, la STS doit conclure avec lui un contrat écrit précisant ce qui suit:
 - a) les obligations de confidentialité du fournisseur;
 - b) la responsabilité du fournisseur quant à la destruction sécuritaire des documents;
 - c) la méthode de destruction des documents (voir l'article 5 plus loin), les conditions de cette destruction et la personne qui en est responsable;
 - d) l'obligation de produire, après la destruction, un certificat comportant la date, l'heure, le lieu et la méthode de destruction ainsi que la signature du responsable;
 - e) la confirmation que les employés du fournisseur comprennent l'importance de la destruction sécuritaire de renseignements personnels et ont reçu une formation à ce sujet;
 - f) l'obligation pour le fournisseur d'aviser la STS à l'avance des travaux confiés à un sous-traitant et de conclure une entente écrite avec le sous-traitant en question lui imposant les mêmes obligations que celles qu'il a envers la STS;
 - g) le moment où les documents de la STS seront détruits et la nécessité de les entreposer dans un endroit sûr entre-temps.

3. **Sélectionner les employés de la STS avec la diligence requise** : Si les documents sont détruits par des employés de la STS, les conditions suivantes doivent être respectées:
 - (a) Les employés doivent suivre une formation sur les méthodes de destruction de documents appropriées et sur l'importance de la destruction sécuritaire des renseignements personnels.
 - (b) La STS doit remettre aux employés des instructions renfermant certaines modalités clés. Ces instructions doivent:

- (i) énoncer les responsabilités des employés concernant la destruction sécuritaire des documents et les obligations relatives à la confidentialité;
- (ii) préciser la méthode de destruction des documents (voir l'article 5 plus loin), les conditions de cette destruction et la personne qui en est responsable;
- (iii) indiquer le moment où les documents seront détruits et la nécessité de les entreposer dans un endroit sûr entre-temps.

4. Destruction de documents: Les documents dont la destruction est autorisée par le gestionnaire (ou son délégué) doivent être détruits comme suit :

- (a) Si le document **n'est pas** confidentiel, il doit être (i) supprimé (s'il est sous forme électronique)¹ ou (ii) mis au recyclage ou à la poubelle pour la collecte ordinaire (s'il est sous forme papier).
- (b) Si le document **est** confidentiel (y compris, sans s'y limiter, ceux qui contiennent des renseignements personnels), il doit être détruit de façon permanente ou effacé de façon irréversible pour qu'il soit impossible de les reconstituer de quelque manière que ce soit. Les documents papier doivent être détruits au moyen d'une déchiqueteuse à coupe croisée (et non à coupe droite, car il est alors possible de reconstituer le document). Les documents électroniques doivent être détruits de manière sécuritaire:
 - (i) soit en endommageant physiquement le dispositif de stockage pour le rendre inutilisable, puis en en disposant;
 - (ii) soit, s'il est préférable de réutiliser le dispositif, en employant un outil de nettoyage de données capable d'effacer de manière irréversible toutes les données s'y trouvant.

Dans un cas comme dans l'autre, les documents papier associés au support électronique (p. ex., les étiquettes de CD) doivent être détruits de manière sécuritaire de la façon prévue pour les documents papier².

5. Tenir un registre de la destruction de documents

- (a) Une liste détaillée de tous les documents détruits doit être dressée et maintenue, pour qu'il soit possible de déterminer ultérieurement quels documents ont été détruits et quel était leur objet.
- (b) Tous les registres de destruction de documents doivent être conservés de façon permanente.

¹ Il y a différentes façons, plus ou moins efficaces, de disposer de renseignements stockés électroniquement (RSE). Ils peuvent être :

1. supprimés – c'est-à-dire que l'espace disque les contenant est libéré et peut être réutilisé, mais ils peuvent être récupérés à l'aide d'outils spéciaux jusqu'à ce qu'ils soient complètement écrasés;
2. écrasés – c'est-à-dire qu'ils sont remplacés par de nouvelles données dans l'espace disque les contenant, mais ils peuvent être partiellement récupérés à l'aide d'outils spéciaux jusqu'à ce qu'ils soient complètement écrasés;
3. physiquement détruits – c'est-à-dire que le support (disque dur, clé USB, CD, etc.) a subi des dommages physiques qui rendent sa lecture impossible.

La STS doit choisir la méthode de disposition qu'elle juge la plus appropriée compte tenu de ses besoins opérationnels (p. ex., il est impossible de détruire physiquement la plupart des dispositifs de stockage, car ils sont réutilisés) et de la gestion des risques (en particulier, les coûts potentiellement élevés devant être engagés dans le cadre d'un litige pour retrouver des RSE supprimés).

²Ces méthodes de destruction sont tirées de la feuille-info « *La destruction sécurisée de renseignements personnels* », publiée par le Commissaire à l'information et à la protection de la vie privée de l'Ontario en décembre 2005, qui présente des pratiques exemplaires sur la destruction de renseignements personnels.