Canadian Judicial Council
Conseil canadien de la magistrature

Modèle de politique pour la classification de l'information judiciaire

Première édition, Septembre 2022

Préparé par le Dr Martin Felsky, Ph. D., J.D. – Conseiller spécial du CCM en technologie de l'information

TABLE DES MATIÈRES

CONTEXTE

Ce modèle de politique fait suite aux initiatives antérieures du Conseil concernant l'information judiciaire. Tous les tribunaux, ainsi que le Conseil, ont convenu que le concept moderne « d'information judiciaire » n'était plus simplement une question de documents judiciaires officiels ou administratifs acquis ou créés de façon intermittente, avec un contenu sur mesure limité, d'une certaine obscurité pratique découlant de son caractère documentaire et de sa facilité de destruction.

Une décennie plus tard, il est encore plus évident et pressant que les tribunaux reconnaissent que « l'information judiciaire » est un concept beaucoup plus vaste et beaucoup plus accessible et durable qu'avant. Par conséquent, en plus des autres responsabilités en matière d'information judiciaire, chaque tribunal doit créer, tenir à jour et examiner une approche systématique pour la protection de l'information judiciaire de nature délicate tout au long de son cycle de vie. Ce modèle de politique propose un cadre dont les tribunaux doivent tenir compte à cette fin et donne des précisions sur la politique 16 du *Plan directeur pour la sécurité de l'information judiciaire* du Conseil[1] :

Politique 16a : Les tribunaux devraient adopter un système de classification permettant l'identification de l'information judiciaire de nature délicate afin de lui assurer une protection spéciale. Les systèmes de classification adoptés devraient être uniformes dans tous les tribunaux afin d'assurer une compréhension commune des exigences en matière de sensibilité et de protection des actifs.

Politique 16b : L'information classifiée ne peut être mise à la disposition d'une personne que lorsque l'auteur de la demande établit que la personne a un « besoin de savoir », que des contrôles de sécurité appropriés sont en place et que l'accès est nécessaire à l'exercice des fonctions officielles du tribunal.

La classification est un jeu d'équilibre perpétuel qui doit protéger l'information de nature délicate sans en restreindre indûment l'accès. Le but de la classification est de s'assurer que le

[1] *Plan directeur pour la sécurité de l'information judiciaire* (6e édition, CCM 2021). En anglais : *Blueprint for the Security of Court Information*. Désormais, Plan directeur.

risque de préjudice découlant d'une atteinte à la sécurité ou à la vie privée est maintenu à un niveau acceptable pour le tribunal, correspondant à sa tolérance au risque, au moyen de la désignation, de l'étiquetage et du traitement appropriés de l'information de nature délicate.

LA CLASSIFICATION N'EST QU'UNE PARTIE DU CONTRÔLE D'ACCÈS

La classification des actifs informationnels guide les détenteurs en ce qui concerne leur traitement et leur diffusion sécuritaire, mais la classification n'est pas la seule mesure de protection limitant l'accès. L'information classifiée ne devrait être mise à la disposition d'une personne que lorsque l'auteur de la demande établit que la personne a un « besoin de savoir » valide, de sorte que l'accès est nécessaire à l'exercice des fonctions officielles du tribunal.

Il existe d'autres restrictions potentielles à l'accès à l'information classifiée, y compris les autorisations de sécurité du personnel et les accords de confidentialité.

DÉFIS

La protection des renseignements de nature sensibles repose en grande partie sur ses auteurs, soit les officiers de la cour, représentants de la cour et le personnel, qui doivent prendre les bonnes décisions de classification à l'égard de chaque courriel ou dossier qu'ils rédigent ou reçoivent. Cette responsabilité peut être lourde, surtout compte tenu du volume de l'information judiciaire à traiter et de la vitesse à laquelle elle se déplace.

La classification de l'information n'est pas une activité ponctuelle. Les classifications de sécurité sont dynamiques et doivent être revues périodiquement, à mesure que le profil de risque du tribunal change, que les capacités de son système ou son architecture changent, ou que la nature des actifs informationnels elle-même change au fil du temps.

Le travail à distance, les audiences virtuelles et l'informatique en nuage font maintenant partie des activités courantes des tribunaux, élargissant la portée des cyber menaces bien au-delà des locaux du palais de justice.

Les tribunaux devraient aborder ces questions en préconisant une approche moderne de la classification. Jusqu'à ce que l'on puisse faire confiance à l'intelligence artificielle pour prendre des décisions fiables en matière de classification de sécurité en notre nom, il existe des mesures

qui permettent d'enlever aux membres du tribunal le fardeau de la classification, mais pas celui du contrôle. Il existe des solutions hybrides qui combinent des processus de classification automatisés et manuels. Les systèmes qui analysent l'information peuvent être configurés de diverses façons pour suggérer des classifications appropriées en fonction du contenu ou du contexte de l'information.

Par exemple, Microsoft 365 offre une fonction d'étiquetage des ressources avec des étiquettes de sensibilité qui peuvent être configurées au préalable par le tribunal. Il est ainsi plus facile pour les utilisateurs d'appliquer (ou simplement de confirmer) des étiquettes lorsqu'ils préparent des courriels et des documents[2].

Les systèmes de prévention de la perte de données (PPD) sont des programmes automatisés qui peuvent agir comme filet de sécurité en cas de manquement de la classification. Ils analysent les communications sortantes, bloquent les communications non autorisées ou avertissent les expéditeurs[3].

Au final, le but d'un système de classification moderne devrait être d'établir les bases d'un logiciel de classification entièrement automatique et artificiellement intelligent.

INDÉPENDANCE JUDICIAIRE

La magistrature jouit d'une indépendance institutionnelle et individuelle, ce qui comporte une couche importante de coopération à la gouvernance de l'information judiciaire. Les tribunaux canadiens sont administrés conjointement par la magistrature et le pouvoir exécutif, et par d'autres administrateurs non judiciaires qui s'occupent de la gestion des installations, des ressources humaines, de l'infrastructure ou de l'approvisionnement. De plus, tout type de renseignements opérationnels que le tribunal juge appropriés à son mandat ou à sa capacité entre dans la catégorie de l'administration judiciaire. Les juges en chef se penchent sur des questions comme le retard dans le jugement, l'équilibrage des charges, la formation et la conduite des juges, le bien-être, la sensibilisation du public, et sur de nombreuses autres questions communes aux tribunaux que les processus opérationnels des « ressources humaines » ne couvrent pas.

[2] Voir Azure Information Protection.
[3] Les systèmes de PPD doivent toujours être configurés en tenant compte des principes d'indépendance judiciaire, mais les officiers judiciaires ne devraient pas être exemptés des règles de classification et des contrôles de sécurité des tribunaux.

Ainsi, même si l'information judiciaire doit respecter des lois générales[4] et des politiques gouvernementales bien établies, elle est également assujettie à des protocoles d'entente négociés individuellement, à la discrétion judiciaire et à la compétence des tribunaux sur son processus et ses dossiers.

Le présent document ne doit pas être interprété de façon à modifier la distinction entre l'information judiciaire qui est exclusivement la propriété et sous le contrôle du tribunal et l'information judiciaire qui, de par sa nature, peut être délégué ou acquise directement ou indirectement par le pouvoir exécutif.

ÉNONCÉS DE LA POLITIQUE

1. OBJET

La présente politique établit un processus officiel de classification des actifs informationnels afin de s'assurer que les contrôles de sécurité de base utilisés pour protéger l'information judiciaire sont proportionnels aux risques d'accès non autorisé. Elle établit des niveaux de classification clairement définis qui peuvent être appliqués de façon efficace et uniforme à toutes les actifs informationnels des tribunaux.

COMMENTAIRE

En fin de compte, la classification de l'information judiciaire vise à prévenir les préjudices aux personnes (y compris les pertes de vie), aux tribunaux ou à d'autres organisations, aux marchés financiers ou au système de justice. Elle protège la vie privée, les privilèges juridiques et le secret judiciaire, ou tout autre type d'information de nature délicate.

Un système de classification assure des responsabilités claires pour la protection adéquate des renseignements des tribunaux. Il aide à prioriser les affectations budgétaires pour les mesures de sécurité, facilite le respect des lois, des ordonnances des tribunaux, des accords de

[4] Parmi les exemples de lois pertinentes, mentionnons le *Code criminel*, les lois sur les secrets officiels, sur les archives et les dossiers publics, sur les infractions provinciales, sur les tribunaux judiciaires, sur la preuve, sur le commerce électronique, sur la protection des renseignements personnels, sur la liberté d'accès à l'information ou sur l'accès à l'information.

confidentialité, des permis et d'autres obligations. Il s'agit d'un moyen important d'identifier les renseignements qui peuvent être transférés en toute sécurité vers un fournisseur de services infonuagiques ou partagés avec des partenaires du système de justice.

2. PORTÉE

La présente politique s'applique à toutes les actifs informationnels des tribunaux, où qu'elles se trouvent et quel que soit le format ou le support avec lequel elles sont transmises ou stockées.

L'information judiciaire qui contient des renseignements personnels identifiables (p. ex. au sujet des plaideurs, des témoins, des juges et du personnel) doit être classifiée en conséquence.

Les documents personnels qui n'ont aucun lien avec les affaires du tribunal sont confidentiels et ne font pas partie des actifs informationnels de la magistrature.

3. GLOSSAIRE

Dossier judiciaire

Un dossier judiciaire contient de l'information directement liée à une seule procédure judiciaire ou à un certain nombre de procédures judiciaires qui portent le même numéro de dossier. Cela comprend l'information inclus dans les documents judiciaires et toute autre information qui a été saisie ou placée dans le dossier judiciaire[5].

Documents judiciaires

L'information et les autres pièces tangibles déposées dans le cadre des procédures, ainsi que l'information concernant ces procédures qui est conservée par la cour[6].

Actif informationnel

[Traduction] « Un actif informationnel consiste en un ensemble de renseignements définis et gérés comme une seule unité afin qu'ils puissent être compris, partagés, protégés et exploités

[5] Voir Conseil canadien de la magistrature, *Définition modèle des renseignements de la magistrature* (2020)
[6] Voir la note 9 de bas de page.

efficacement. Un actif informationnel comporte une valeur, des risques, du contenu et un cycle de vie reconnaissables et gérables[7]. »

Les actifs informationnels peuvent être physiques (comme les documents au format papier, les films, les impressions photographiques) ou numériques, donc stockées électroniquement. Des exemples de ressource d'information sont un document au format papier ou une boîte de documents, une feuille de calcul, le contenu d'un lecteur réseau partagé, une base de données, un système d'exploitation, un système de classement électronique, un fichier PDF téléchargé dans un tel système, un dossier judiciaire, des documents judiciaires, un courriel ou un compte de courriel en entier.

Selon le contexte, il se peut que certains tribunaux classent les objets constituant des éléments de preuve physiques non documentaires (par exemple les prélèvements médico-légaux) comme des actifs informationnels.

Gardien

Personne ou unité opérationnelle responsable de la mise à jour des systèmes de communication et de la technologie utilisés pour l'information judiciaire.

Fournisseur

Personne ou organisation externe qui soumet ou transfère des actifs informationnels au tribunal.

4. RÔLES ET RESPONSABILITÉS

Contrôleur de l'information

Le contrôleur de l'information a le contrôle légal des actifs informationnels. Un tel contrôle est dissocié de la notion de garde ou possession physique[8]. Les contrôleurs de l'information (ou

[7] UK National Archives factsheet (fiche d'information des archives nationales du Royaume-Uni).

[8] Il est important de garder à l'esprit les distinctions faites à la page 6 du rapport suivant du CCM publié en 2013 *Cadre de politique de gestion de l'information judiciaire dans le monde numérique*, Conseil canadien de la magistrature: Dans le monde imprimé, la propriété d'un dossier de tribunal est synonyme de contrôle de ce dossier. Il est facile pour la magistrature de contrôler les dossiers dans un tel environnement, parce qu'un dossier de tribunal original ne peut se trouver qu'à un seul endroit physique à la fois et que les personnes en possession du dossier physique peuvent facilement contrôler l'accès à l'information que celui-ci contient.
Dans le monde numérique, cependant, il est tout à fait possible de posséder de l'information sans toutefois la contrôler et, inversement, il est possible de contrôler de l'information sans en avoir la possession physique.

responsables de données) définissent les politiques d'information générales régissant l'accès, l'utilisation et la conservation des actifs informationnels.

Les contrôleurs sont responsables de déterminer la classification des actifs informationnels de la magistrature qu'ils contrôlent et sont autorisés à approuver les demandes d'accès ou de déclassement. Les contrôleurs peuvent exiger des contrôles de sécurité supplémentaires de façon *ponctuelle* ou renforcer les protocoles de traitement de l'information au besoin.

Auteur

L'auteur est une personne ou une unité opérationnelle du tribunal qui rédige ou reçoit de l'information judiciaire. Les auteurs sont responsables d'examiner et d'appliquer les étiquettes de classification aux ressources qu'ils créent ou reçoivent, conformément à la présente politique et aux autres directives du tribunal.

Agent de la sécurité informatique du système judiciaire

L'agent de la sécurité informatique du système judiciaire (ou tout autre agent qualifié nommé par le tribunal) est responsable de l'administration de la présente politique. L'agent de la sécurité informatique du système judiciaire met périodiquement à jour le registre des actifs informationnels (politique 6) et assure la conformité au moyen de fonctions d'examen et de vérification régulières. Une formation sur le traitement de l'information classifiée doit être donnée régulièrement à tous les utilisateurs.

Utilisateurs

Toute personne ayant accès à l'information judiciaire est un utilisateur. Les utilisateurs doivent suivre une formation et respecter toutes les politiques et procédures relatives au traitement de l'information judiciaire classifiée.

5. TRANSITION

La présente politique entre en vigueur dès son approbation par le tribunal.

COMMENTAIRE

Cette politique peut être mise en œuvre progressivement, au jour le jour. Les ressources existantes peuvent être classifiées au fil du temps, en priorité selon la durée de leur période de conservation.

6. REGISTRE DES ACTIFS INFORMATIONNELS

Le tribunal doit préparer et mettre à jour un registre des actifs informationnels (RAI) qui énumère, décrit brièvement et catégorise toutes les actifs informationnels de la magistrature.

COMMENTAIRE

Le RAI est le premier pas à franchir pour prendre le contrôle de l'information judiciaire. Voici les éléments clés à prendre en considération pour l'enregistrement de chaque catégorie de ressource :

1. Une brève description comprenant le but et l'utilisation des actifs
2. Les dates de début et de fin
3. Le contrôleur (avec coordonnées)
4. Le gardien (avec coordonnées)
5. Les utilisateurs, partage à l'interne ou à l'externe
6. L'emplacement – nuage, sur place, base de données, dépôt, domaine
7. Le formulaire – papier, électronique ou autre format ou moyen
8. La protection de l'information – par exemple, droit d'auteur, vie privée, privilège, confidentialité
9. Devrait-il s'agir d'une ressource désignée[9]?

Dans la profession de la gouvernance de l'information, il est bien établi que, pour l'information numérique, il est plus logique d'avoir des catégories plus vastes et plus inclusives, car cette

[9] Le RAI constitue une base non seulement pour la prise de décisions quant à la classification, mais aussi sur l'évaluation des menaces et des risques, sur la conservation et la disposition de l'information judiciaire et sur les procédures de continuité des activités. La désignation des actifs dans cette liste est pertinente à des fins de conservation. Voir le *Modèle de politique sur la conservation de l'information judiciaire* du Conseil canadien de la magistrature (2022).

information est dynamique et souvent stockée dans des dépôts non structurés plutôt que dans des dossiers distincts. La quantité de ressources qui doivent être énumérées et suivies individuellement augmente avec le niveau de détail et de précision du RAI. Pensons, par exemple, à une liste par nom de document.

Bien que l'établissement de regroupements de haut niveau simplifie le processus de classification, certaines ressources nécessiteront une classification détaillée. Par exemple, un seul champ ou enregistrement dans une base de données, ou un formulaire ou un fichier particulier peut contenir des renseignements qui nécessitent une classification différente de celle du groupe qui lui a été attribué. La conception créative peut être nécessaire pour attribuer des classifications détaillées, par exemple dans une base de données, où certains groupes de dossiers ou de champs dans la même base de données peuvent nécessiter des classifications différentes. Ces conceptions sont limitées par les caractéristiques de sécurité et les contrôles intégrés à chaque système.

Les actifs peuvent être regroupés de façons différentes. Cela dépend du mandat, de la taille et de l'environnement technologique du tribunal. En général, les méthodes suivantes sont utilisées :

- ***Contenu***, qui regroupe l'information selon son sens ou son but
- ***Contexte***, qui regroupe l'information par unité opérationnelle, fonction, système ou plateforme
- ***Utilisateur***, qui regroupe l'information par personne, poste ou rôle au tribunal.

7. ÉVALUATION DES RISQUES

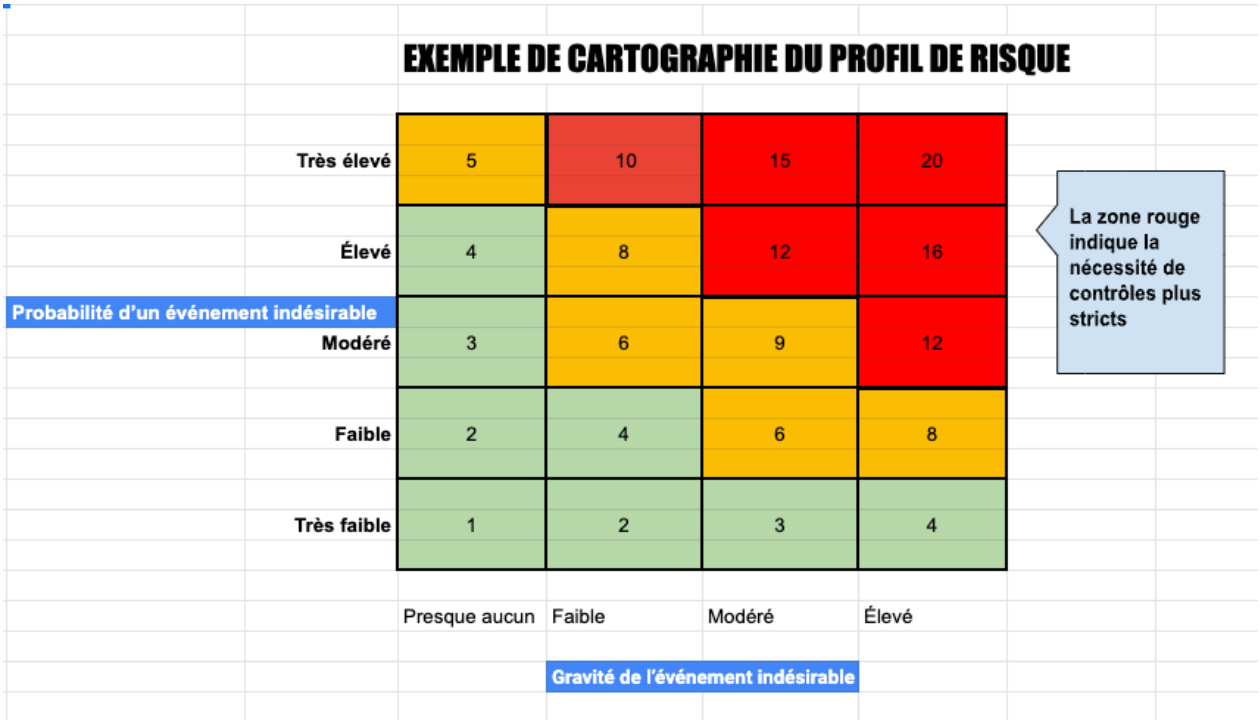
Le tribunal doit planifier, réaliser et prendre en considération les résultats d'une évaluation de la menace et des risques (EMR) afin de déterminer les classifications appropriées pour chaque groupe des actifs informationnels dans le RAI[10].

COMMENTAIRE

L'EMR aide le tribunal à évaluer le degré de préjudice qui pourrait raisonnablement résulter d'une divulgation non autorisée. Un schéma simplifié est présenté ci-dessous. Les risques identifiés sont évalués en ce qui concerne la probabilité et le préjudice. Le tableau qui en résulte

[10] Voir Politique du Plan directeur 3b.

fournit aux décideurs une base pour déterminer le profil de risque du tribunal, les contrôles de sécurité proportionnels et les désignations de classification. Le rapport d'EMR indique également les risques résiduels qui doivent être abordés pour atteindre un niveau de risque acceptable pour le tribunal.



8. CLASSIFICATION DES ACTIFS INFORMATIONNELS

Toute l'information judiciaire doit être classifiée en fonction de la nature délicate de son contenu et des risques associés à la divulgation et à l'accès non autorisés.

L'information copiée, extraite, imprimée ou qui est autrement dérivée d'une information classifiée a la même classification que l'information d'origine.

Il faut utiliser les classifications suivantes :

PUBLIC

S'applique à l'information qui, si elle était compromise, présenterait peu ou pas de risque pour une personne, le tribunal ou une autre organisation. L'information peut être rendue publique, car la divulgation n'aurait pas d'effet négatif prévu, ou est exigée par la loi. Par exemple : comptes

rendus des délibérations, rapports annuels, listes des audiences et registres de la Cour.

CONFIDENTIEL[11]

S'applique à l'information qui, si elle est compromises, pourrait causer un préjudice à une personne, au tribunal ou à une autre organisation[12]. L'accès interne et externe est limité aux personnes ou aux organisations qui ont un besoin justifié de savoir. Par exemple : politiques et directives internes; courriels courants, exposés de cas et notes de service de conférence de cas.

RESTREINT

S'applique à l'information qui, si elle est compromise, pourrait causer un préjudice sérieux à une personne, au tribunal ou à une autre organisation[13]. L'accès interne est limité. L'accès externe est assujetti à l'ordonnance du tribunal, à la législation, à la politique du tribunal, aux règles du tribunal, à l'autorisation de sécurité approuvée par le tribunal et à l'accord de confidentialité. Accès et actions à consigner. Par exemple, les projets de jugement et les connaissances d'office; les décisions, les endossements et les projets d'accusations devant jury; les documents et ordonnances assujettis à une interdiction de publication et les enregistrements numériques d'une instance fermée ou scellée. L'information judiciaire restreinte serait sujette à un traitement plus rigoureux que celles confidentielles, qui inclurait un étiquetage particulier, le chiffrement et l'entreposage sur des supports désignés. Toute cette information doit être clairement et visiblement étiquetée « RESTREINT ».

SECRET

S'applique à l'information qui, si elle est compromise, pourrait causer un préjudice extrêmement grave à une personne, au tribunal ou à une autre organisation[14]. L'accès est limité aux personnes désignées et autorisées qui ont besoin de savoir ou qui ont conclu un accord de confidentialité, ou encore en cas d'ordonnance du tribunal. Tous les accès et les actions doivent être consignés. Par exemple, les renseignements du gouvernement, les dossiers scellés et les renseignements

[11] Cela s'écarte de la suggestion du Plan directeur, dans lequel la désignation « Officiel » a été proposée. Toutefois, comme le mot « officiel » pourrait être utilisé pour désigner certains types de dossiers judiciaires à des fins autres que la sécurité, le terme « confidentiel » est préférable ici.
[12] Correspond au Protégé A du Canada.
[13] Correspond au Protégé B du Canada.
[14] Correspond au Protégé C du Canada

concernant les informateurs. Toute cette information doit être clairement et visiblement étiquetée « SECRET ». (Les marques de source d'origine doivent également être laissées en place.)

COMMENTAIRE

Chaque actif informationnel du tribunal doit être classé selon le niveau approprié à l'information la plus délicate de sa catégorie. Les actifs informationnels devraient être classées au niveau le plus bas possible, mais aussi élevées que nécessaire. Cette dynamique représente l'équilibre critique à atteindre entre le préjudice qui pourrait être causé par un accès non autorisé et les avantages de l'accès au tribunal, aux parties ou au public.

Une classification excessive entraîne une augmentation des coûts de maintenance, restreint l'accès légitime et peut encourager certains utilisateurs à échapper aux contrôles de sécurité.

Les mots descriptifs comme « Confidentiel » et « Secret » sont plus significatifs et sont donc préférés à un langage abstrait comme « Protégé A » ou « Niveau 3 ». Indépendamment de leurs étiquettes, cependant, le système de classification de l'information judiciaire à quatre niveaux de cette politique s'harmonise avec les systèmes de classification des gouvernements fédéral et provinciaux canadiens, ce qui réduit la confusion pour le personnel des tribunaux qui travaille régulièrement avec l'information du gouvernement et judiciaire. Dans les tribunaux spécialisés, des niveaux de classification plus élevés peuvent être nécessaires pour peaufiner le traitement des données de nature délicate reçues de fournisseurs comme les gouvernements étrangers.

Une façon d'éclaircir les différences entre les trois classifications sécurisées est de montrer aux utilisateurs que la divulgation de renseignements secrets causerait environ dix fois plus de dommages que la divulgation de renseignements à diffusion restreinte, et la divulgation de renseignements à diffusion restreinte causerait environ dix fois plus de dommages que la divulgation de renseignements confidentiels[15].

Les auteurs doivent savoir que la compilation d'information classifiée de faible niveau pourrait, dans de rares cas, mener à la compilation exigeant une classification plus élevée. Cela s'explique par la possibilité que la compilation révèle une relation ou une tendance qui devrait être classifiée à un niveau plus élevé que ses composantes.

[15] Voir Quist, *Security Classification of Information*, volume 2, chapitre 7.

9. INFORMATION DÉJÀ CLASSIFIÉE

L’information qui a été classifiée ailleurs doit être classifiée par le tribunal à un niveau correspondant à celui du fournisseur et être traitée conformément aux contrôles du fournisseur dans la mesure où la classification est plus sévère que celle du tribunal.

L’information reçue d’organisations externes doit être protégée conformément à toute exigence législative ou réglementaire pertinente, y compris les ententes et obligations internationales.

COMMENTAIRE

Lorsque le tribunal reçoit de l'information classifiée par un fournisseur, il doit suivre les règles applicables à cette classification.

10. DÉCLASSEMENT DES CLASSIFICATIONS

Les contrôleurs de l'information peuvent déclasser l'information qu'ils contrôlent.

Les auteurs (ou leurs successeurs) peuvent déclasser leurs propres actifs informationnels.

Les utilisateurs ne peuvent pas déclasser un actif informationnel sans l'approbation de son auteur ou du contrôleur.

COMMENTAIRE

La classification des ressources peut être mise à niveau ou déclassée au besoin, avec l'autorisation appropriée. Au fil du temps, les classifications d'un document ou d'un autre actif peuvent être modifiées en fonction d'un délai expiré, d'un certain événement ou d'une réévaluation de routine.

11. ÉTIQUETAGE DE L'INFORMATION CLASSIFIÉE – BANNIÈRES

Toutes les ressources (y compris les copies et les impressions) doivent être étiquetées avec une bannière indiquant leur niveau de classification.

La bannière comprend le nom (ou l'abréviation) du tribunal et le niveau de classification en MAJUSCULES. Par exemple :

Exemple de bannière de classification (options)	
Conseil canadien de la magistrature – CONFIDENTIEL	CCM – CONFIDENTIEL

Au moment de la classification d'origine, la bannière doit être affichée clairement et visiblement sur le dessus et sur chaque page de l'actif, par exemple les en-têtes et pieds de page, ou si

l'information n'est pas propice à un tel marquage, la désignation de classification doit être clairement associée à son sujet d'une manière adaptée à sa forme. Lorsqu'il n'est pas pratique d'appliquer une marque, les utilisateurs doivent être informés de la désignation de classification et de tout traitement spécial requis.

Si des parties d'un document ont des classifications différentes, chaque partie doit être étiquetée de façon appropriée pour indiquer son niveau de classification.

COMMENTAIRE

La bannière de classification est le principal mécanisme par lequel la sensibilité d'un actif informationnel est affiché. Un aspect clé d'une étiquette de classification est qu'elle est comme un passeport, il s'agit d'une pièce d'identité importante qui doit accompagner la ressource lors de ses déplacements. Peu importe la méthode utilisée pour apposer une étiquette, elle doit être visible, lisible et tenace.

Lorsque les classifications sont prédéterminées, elles peuvent être ajoutées aux modèles de documents. Pour les courriels, la classification doit être indiquée dans la ligne d'objet et, éventuellement, dans le corps du courriel. Les signatures de courriel peuvent également contenir un marquage de classification, ce qui fonctionne bien lorsque les politiques sont appliquées par l'utilisateur ou le groupe d'utilisateurs. De préférence, les systèmes de courriel devraient être configurés de manière à contraindre les utilisateurs à sélectionner une classification avant l'envoi, par exemple dans un menu déroulant.

12. ÉTIQUETAGE DE L'INFORMATION CLASSIFIÉE – BLOC

En plus de la bannière, les actifs informationnels classifiés peuvent être marqués d'un bloc d'information facultatif. L'objectif est de fournir aux utilisateurs de plus amples renseignements sur l'état de l'actif. Le bloc doit être affiché sur le dessus de chaque document classifié, ou autrement d'une manière bien en vue adaptée à la forme de l'actif informationnel.

L'exemple ci-dessous montre le type d'information qu'un bloc pourrait contenir :

Classifié par : L'hon. juge en chef Moreau
Raison : Preuve scellée
Déclassification : Sur ordonnance du tribunal
Restrictions de diffusion supplémentaires : Aucune

COMMENTAIRE

En fournissant le nom de l'autorité de classification (contrôleur ou auteur), les utilisateurs savent avec qui communiquer en cas de proposition de reclassification. La justification de la classification est utile à des fins de vérification et de conformité. Si une date ou un événement de déclassification peut être déterminé au moment de la création de l'actif informationnel, cela aide les utilisateurs à prendre des décisions au sujet de la diffusion. D'autres restrictions peuvent être utiles dans diverses circonstances, par exemple lorsqu'il s'agit de traiter des ressources classifiées par des fournisseurs qui nécessitent plus que les contrôles établis[16].

13. TRAITEMENT DES ACTIFS INFORMATIONNELS CLASSIFIÉS

Toute l'information judiciaire doit être traitée conformément à sa classification et aux procédures établies dans le guide de classification. (Voir l'annexe 1.)

Lorsque de l'information judiciaire classifiée est transférée à un tiers, le tribunal doit s'assurer que les politiques et les procédures de sécurité du tiers sont suffisamment robustes pour respecter les contrôles de classification requis.

[16] L'accès à l'information judiciaire n'est pas déterminé par la seule classification. Les droits d'accès sont plutôt déterminés par une combinaison de contrôles fondés sur la classification, le filtrage ou l'habilitation de sécurité individuelle et par la fonction ou le travail assigné de la personne, qui détermine son besoin de savoir.

ANNEXE 1 – GUIDE DE CLASSIFICATION

Les tableaux ci-dessous sont des exemples destinés à servir de guide et ne sont ni définitifs ni exhaustifs. Vous pouvez consulter la liste des références ci-dessous si d'autres approches ou exemples sont nécessaires.

TABLEAU 1 : CARTOGRAPHIE DES RISQUES ET DE L'ACCÈS

Classification	Niveau de risque	Description du risque	Accès
Public	Presque aucun	S'applique à l'information ou à l'actif informationnel qui, s'il était compromis, présenterait peu ou pas de risque pour une personne, le tribunal ou une autre organisation.	L'information peut être rendue publique.
Confidentiel	Faible	S'applique à l'information ou à l'actif informationnel qui, si il était compromis, pourrait causer un préjudice à une personne, au tribunal ou à une autre organisation.[17]	L'information peut être communiquée à l'interne et à des tiers ayant un besoin légitime de savoir.
Restreint	Modéré	S'applique à l'information ou à l'actif informationnel qui, si il était compromis, pourrait causer un préjudice sérieux à une personne, au tribunal ou à une autre organisation.[18]	L'accès interne est limité. Accès externe assujetti à l'autorisation de sécurité approuvée par le tribunal et à l'accord de confidentialité. Accès et actions à consigner.
Secret	Élevé	S'applique à l'information ou à l'actif informationnel qui, si il était compromis, pourrait causer un préjudice extrêmement grave à une personne, au tribunal ou à une autre organisation[19].	L'accès est limité aux personnes désignées et autorisées qui ont besoin de savoir et qui ont conclu un accord de confidentialité. Tous les accès et les actions doivent être consignés.

[17] Correspond au niveau fédéral Protégé A. Voir https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html.
[18] Correspond au niveau fédéral Protégé B. Voir https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html.
[19] Correspond au niveau fédéral Protégé C. Voir https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html.

TABLEAU 2 : CONTRÔLES DES ÉCHANTILLONS

Classification	En arrêt (entreposage)	En transit	Destruction
Public	Peut être stocké sur des dispositifs amovibles et un service infonuagique public.	Aucun contrôle spécial	Aucune exigence spéciale de suppression.
Confidentiel	• Toutes les politiques de sécurité de base du Plan directeur[20] sont en place. • Sur place, doit être stocké sur le réseau du tribunal avec des contrôles d'accès basés sur les dossiers (et sauvegardés). • Peut être stocké dans un service infonuagique public approuvé par le tribunal. • Peut être stocké sur des dispositifs amovibles seulement s'il est chiffré à l'aide d'outils approuvés par le tribunal. • Les contrôles techniques à ce niveau seront basés sur des produits et services assurés et disponibles sur le marché, sans besoin de personnalisation. • Les renseignements inactifs seront protégés par défaut. Les données ne doivent être transmises que par un réseau sécurisé. • Les données qui traversent un réseau non fiable (non sécurisé) doivent comprendre une cryptographie conforme aux normes de l'industrie.	Utiliser uniquement les courriels, les messages textes et les autres plateformes de communication approuvés par le tribunal.	L'information devrait être purgée à l'aide des outils conformes aux normes de l'industrie.
Restreint	• Politiques de sécurité améliorées[21] du Plan directeur. • Peut être stocké dans un service infonuagique public approuvé par le tribunal. • L'accès nécessite une authentification multifactorielle. • Peut être stocké sur des dispositifs amovibles seulement s'il est chiffré à l'aide d'outils approuvés par le tribunal.	L'information doit être chiffrée au moyen d'outils approuvés par le tribunal.	L'information devrait être purgée à l'aide des outils conformes aux normes de l'industrie.
Secret	• Exige le niveau le plus élevé de contrôles de sécurité raisonnablement disponibles.	Ne pas transmettre par courriel ou par tout autre	Les renseignements doivent être purgés de

[20] Les tribunaux devraient consulter le Plan directeur pour obtenir des détails sur le contrôle de l'accès, la sécurité physique et d'autres contrôles.
[21] Les tribunaux devraient consulter le Plan directeur pour obtenir des détails sur le contrôle de l'accès, la sécurité physique et d'autres contrôles.

Classification	En arrêt (entreposage)	En transit	Destruction
	• Tous les accès doivent être consignés et faire l'objet d'un suivi (sous réserve des lignes directrices sur la surveillance)[22]. • Ne peut pas être stocké sur des dispositifs amovibles. • Ne convient pas à l'hébergement sur un service infonuagique public. • Les entrepôts de données devraient être déconnectés de l'Internet public. • Les fichiers électroniques ou les données doivent être stockés dans un répertoire partagé par le tribunal ou un appareil fixe (c.-à-d. un ordinateur de bureau ou un serveur) avec un accès physique contrôlé et des contrôles d'accès logique selon les postes. • Les fichiers électroniques ou les données doivent être chiffrés lorsqu'ils sont stockés sur des appareils portatifs ou non sécurisés. • Les renseignements confidentiels ou de nature délicate communiqués à des tiers doivent être chiffrés au moyen de fichiers. • Les appareils portatifs ou non sécurisés doivent être entreposés dans un endroit sûr lorsqu'ils ne sont pas utilisés.	moyen sur les réseaux publics. Échanger seulement au moyen de mécanismes sécurisés appropriés. Il sera nécessaire d'utiliser des services partagés dûment approuvés avec un cryptage de haut niveau. L'information ne sera communiquée qu'aux utilisateurs désignés.	façon définitive; il pourrait être nécessaire de détruire physiquement les dispositifs d'entreposage. Les données et les supports doivent être démagnétisés (essuyés magnétiquement) ou rendus illisibles par d'autres moyens. Les dispositifs peuvent être physiquement détruits.

[22] Reproduit dans le Plan directeur.

TABLEAU 3 : MARQUAGE DE L'INFORMATION CLASSIFIÉE

Les jours des timbres en caoutchouc sont comptés, tout comme ceux des enveloppes de papier manille et des cachets de cire. L'information numérique n'est pas toujours sous la forme d'un document de traitement de texte auquel les en-têtes et les pieds de page peuvent être facilement appliqués. Ce tableau présente des exemples de méthodes de marquage de l'information numérique. Toute méthode utilisée doit être appropriée au format de l'actif informationnel et doit indiquer clairement à l'utilisateur final que l'information a été classifiée.

Format	Marquage
Courriel ou message texte	Insérer la bannière de l'étiquette dans la ligne d'objet. Si ce n'est pas possible, l'insérer dans le haut du corps du courriel ou de l'espace de signature.
Fichier texte ou image	Insérer l'étiquette dans les métadonnées, sur toutes les images, ou dans l'en-tête, le pied de page ou le filigrane.
Base de données	Insérer l'étiquette dans l'en-tête, le pied de page ou le filigrane des rapports générés, et dans les métadonnées pour chaque enregistrement, champ ou rapport.
Audio	Insérer l'information sonore sur la classification au début du fichier.
Vidéo	Insérer l'information sonore sur la classification au début du fichier. Insérer une étiquette de classification visible sur chaque cadre.

TABLEAU 4 : EXEMPLES DE RENSEIGNEMENTS CLASSIFIÉS DES TRIBUNAUX

Veuillez noter que ces listes sont tirées de plusieurs ressources publiques et internes à titre d'exemples seulement et ne sont ni définitives ni exhaustives. Elles sont simplement représentatives du type d'information qui pourrait figurer dans le cadre de classification d'un tribunal.

Classification	Exemples
Public	• Historique de la liste de cas • Plaidoiries • Ordonnances et motifs de jugement • Transcriptions de procès • Liste des districts judiciaires • Rapports annuels • Formulaires, règles et directives de pratique ou notes • Noms des juges et dates de nomination
Confidentiel	• Politiques et directives internes • Établissement du calendrier des officiers judiciaires et des audiences • Information sur le perfectionnement professionnel • Dossiers des réunions du personnel (autres que l'administration judiciaire) • Directives au jury • Courriels courants et autres communications • Dossier du tribunal/dossier de cause non assujetti à une ordonnance de mise sous scellés
Restreint	• Projets de jugements, de décisions et d'approbations • Décisions définitives des tribunaux si elles sont assujetties à une ordonnance de non-publication • Enregistrement numérique d'une procédure fermée • Notes de recherche, notes judiciaires • Mandats non exécutés, pardons • Ordres du jour, notes et procès-verbaux de réunions concernant l'administration de la justice • Renseignements sur l'administration du personnel • Renseignements sur les juges • Renseignements obtenues par autorisation judiciaire (documents scellés, protection de l'enfance et de la jeunesse)

Classification	Exemples
Secret	• Certains projets de jugement • Renseignements personnels des officiers judiciaires • Demandes de mandat de perquisition et de saisie, surveillance électronique et documents correspondants • Renseignements sur les informateurs • Évaluations psychiatriques • Renseignements personnels des juges • Documents privilégiés • Renseignements liés à la sécurité nationale