CJC CCM
Canadian Judicial Council
Conseil canadien de la magistrature

Modèle de politique pour la classification de l'information judiciaire

Deuxième édition, septembre 2023

Préparé par Martin Felsky, Ph.D., J.D.

TABLE DES MATIÈRES

CONTEXTE ET OBJET

Ce modèle de politique fait suite aux initiatives prises par le Conseil en 2013 en matière d'information judiciaire[1], y compris le *Plan directeur pour la sécurité de l'information judiciaire* (Plan directeur)[2] et les *Lignes directrices sur la migration de l'information judiciaire vers un fournisseur de services d'informatique en nuage*. Toutes les cours, de même que le Conseil, ont reconnu que le concept moderne « d'information judiciaire » ne se limitait plus aux documents judiciaires administratifs acquis ou créés de façon intermittente, lesquels ont peu de contenu adapté et revêtent une certaine obscurité pratique en raison de leur nature documentaire.

Une décennie plus tard, il est encore plus évident et pressant que les cours doivent reconnaître que « l'information judiciaire » est un concept beaucoup plus vaste et qu'elle est beaucoup plus accessible et durable qu'auparavant. Par conséquent, et en plus de ses autres responsabilités en matière d'information judiciaire, chaque cour doit adopter, maintenir et revoir une approche systématique de la vérification et de la réglementation du cycle de vie de l'information judiciaire. Il est recommandé que les cours songent aussi à établir des politiques sur la création, la saisie, la tenue à jour, la conservation et la disposition de l'information judiciaire, en lien avec un accord conceptuel sur la classification.

Cette deuxième édition du modèle de politique est très semblable à la première, mais elle est mieux alignée sur les vues du Conseil concernant les principes de la gouvernance de l'information et de l'indépendance judiciaire. Quelques changements ont aussi été faits au texte pour y apporter des précisions.

Certains termes définis dans le document du Conseil intitulé *Définition modèle des renseignements de la magistrature* (Définition modèle)[3] sont employés dans le modèle de politique, mais celui-ci ne doit pas être interprété comme modifiant les distinctions faites dans le Plan directeur. Le modèle de politique donne des précisions sur la politique 16 du Plan directeur :

[1] L'information judiciaire est l'information reçue, recueillie, stockée, utilisée ou produite par une cour aux fins de sa mission (Définition modèle).
[2] En anglais : *Blueprint for the Security of Court Information*.
[3] En anglais : *Model Definition of Judicial Information*.

Politique 16a : Les cours devraient adopter un système de classification permettant d'identifier l'*information judiciaire* sensible pour lui assurer une protection spéciale. Les systèmes de classification adoptés devraient être uniformes parmi l'ensemble des cours, afin d'assurer une compréhension commune des exigences en matière de sensibilité et de protection des actifs.

Politique 16b : L'information classifiée peut être communiquée à une personne seulement si l'auteur de cette information confirme que la personne est autorisée à l'obtenir (« besoin de savoir »), si les mesures appropriées de sécurité du personnel sont en place, et si l'accès à cette information est nécessaire à l'exécution des fonctions officielles de la cour.

La classification est un jeu d'équilibre perpétuel qui aide à protéger l'information sensible sans en restreindre indûment l'accès. La classification a pour but de s'assurer que le risque de préjudice découlant d'une atteinte à la sécurité ou à la vie privée est maintenu à un niveau acceptable correspondant à la tolérance au risque de la cour, en veillant à ce que l'information judiciaire soit désignée, marquée et traitée de manière appropriée.

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

La classification d'un actif d'information sert à guider les utilisateurs pour qu'ils sachent comment le traiter et le diffuser de façon sécuritaire, mais l'accès à l'information judiciaire n'est pas déterminé seulement par sa classification. Les droits d'accès sont plutôt déterminés par des contrôles basés sur la classification, une évaluation ou une autorisation de sécurité individuelle, des accords de non-divulgation, ainsi que les fonctions d'une personne ou les tâches qui lui sont confiées, ce qui permet de déterminer si cette personne a un besoin de savoir.

L'accès à l'information classifiée ne devrait être autorisé que lorsque le responsable de la classification détermine qu'une personne a un « besoin de savoir » valable, c'est-à-dire que l'accès à cette information est nécessaire à l'exercice de ses fonctions judiciaires officielles.

DÉFIS

La protection de l'information sensible repose en grande partie sur les auteurs de cette information, c'est-à-dire les officiers judiciaires, les fonctionnaires de justice et le personnel de la cour, qui doivent prendre les bonnes décisions de classification concernant chaque courriel ou

document qu'ils rédigent ou reçoivent. Cette responsabilité peut être lourde, surtout compte tenu du volume d'information numérique dont traitent les cours et de la vitesse à laquelle cette information est transmise.

La classification de l'information n'est pas une activité qui est accomplie une seule fois. Les classifications de sécurité sont dynamiques et doivent être revues périodiquement, à mesure que le profil de risque de la cour change, que les capacités ou l'architecture de son système évoluent, ou que la nature des actifs d'information eux-mêmes change au fil du temps.

Le travail à distance, les audiences virtuelles et l'informatique en nuage font maintenant partie des activités courantes des cours, ce qui élargit la portée des menaces informatiques bien au-delà des palais de justice.

Les cours devraient faire face à ces questions en adoptant une approche moderne de la classification. Jusqu'à ce qu'on puisse s'en remettre à l'intelligence artificielle pour prendre des décisions fiables en matière de classification de sécurité à notre place, des mesures peuvent être prises pour enlever aux utilisateurs individuels 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 de marquage de l'information à l'aide d'étiquettes de sensibilité qui peuvent être préconfigurées par la cour. Il est ainsi plus facile pour les utilisateurs d'appliquer (ou simplement de confirmer) des étiquettes lorsqu'ils préparent des courriels et des documents[4].

Les systèmes de prévention de la perte de données (PPD) sont des programmes automatisés qui peuvent servir de filet de sécurité en cas d'erreur de classification. Ils analysent les

[4] Voir Azure Information Protection.

communications sortantes, bloquent les communications non autorisées ou avertissent les expéditeurs[5].

En fin de compte, le but d'un système de classification moderne devrait être d'établir les bases d'un logiciel de classification entièrement automatique et doté d'une intelligence artificielle.

INDÉPENDANCE JUDICIAIRE

La magistrature jouit d'une indépendance institutionnelle et individuelle. Dans le cadre de son indépendance institutionnelle, elle exerce un contrôle exclusif sur les renseignements de la magistrature. Ce contrôle comprend le pouvoir inhérent de régir l'accès aux renseignements de la magistrature, de même que l'utilisation, la conservation et la disposition de ces renseignements. En ce sens, le contrôle est distinct des concepts du contrôle physique, de la garde ou de la possession[6], lesquels n'ont pas préséance sur le pouvoir de surveillance des renseignements de la magistrature exercé par les cours. Le présent modèle de politique ne diminue en rien et n'exclut pas la nécessité de séparer et de protéger les renseignements de la magistrature de manière appropriée.

L'organe judiciaire et l'organe exécutif administrent les cours canadiennes conjointement. Par exemple, l'information contenue dans le dossier judiciaire est la responsabilité des deux organes. La consultation, la coordination et la collaboration sont essentielles en ce qui a trait à la conservation de l'information judiciaire.

Il est également nécessaire de veiller à ce que des accords appropriés soient conclus avec l'organe exécutif pour s'assurer que les décisions en matière de classification de l'information judiciaire sont comprises et respectées par tous ceux et celles qui ont accès à cette information.

---

[5] Les systèmes de PPD doivent toujours être configurés en tenant compte des principes de l'indépendance judiciaire, mais les officiers judiciaires ne devraient pas être exemptés des règles de classification et des contrôles de sécurité des cours.

[6] Cette distinction est expliquée à la page 6 du rapport *Cadre de politique de gestion de l'information judiciaire dans le monde numérique*, publié par le CCM en 2013 : « Dans le monde imprimé, la *propriété* d'un dossier de la cour 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 cour 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. ».

La Colombie-Britannique a créé une matrice d'attribution des responsabilités[7] qui pourrait être utile à d'autres cours. Cette matrice précise les différents niveaux de participation dans les cas où la responsabilité de la gouvernance de l'information est partagée. En voici un exemple tiré de la Cour d'appel de la Colombie-Britannique :

Qui doit rendre compte? – Le juge en chef, le registraire de la Cour d'appel et le sous-procureur général ont le pouvoir d'approbation.

Qui est responsable? – Le gestionnaire des documents de la Cour d'appel (l'archiviste) ou l'avocat-conseil de la Cour d'appel (ils font aussi des recommandations).

Qui est consulté? – La Direction des services judiciaires, le Service des documents du gouvernement de la Colombie-Britannique, les Archives de la Colombie-Britannique, le Musée royal de la Colombie-Britannique.

Qui est informé? – Le public, le personnel judiciaire des cours supérieures, le personnel de la Direction des services judiciaires.

La magistrature et l'organe exécutif doivent se consulter pour gérer les coûts de base et les coûts accessoires élevés de la gouvernance de l'information, y compris la classification. Il peut y avoir des coûts liés à la dotation, aux logiciels et à la formation qui ne sont pas présentement inclus dans les budgets de nombreuses cours.

ÉNONCÉS DE POLITIQUE

POLITIQUE 1 – OBJET

La présente politique établit un processus officiel de classification des actifs d'information 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 présente des niveaux de classification clairement définis qui peuvent être appliqués de façon efficace et cohérente à tous les actifs d'information judiciaire.

COMMENTAIRE

[7] Aussi appelée graphique RACI, qui signifie *Responsible, Accountable, Consulted and Informed* (responsable, redevable, consulté et informé).

En définitive, la classification de l'information judiciaire vise à éviter de causer un préjudice aux personnes (y compris la perte de vie), aux cours, à d'autres organisations, aux marchés financiers et au système de justice. Elle sert à protéger la vie privée, les privilèges juridiques et le secret du délibéré, ou n'importe quel type d'information sensible.

Un système de classification définit clairement les responsabilités pour assurer la protection adéquate de l'information judiciaire. Il aide à prioriser les affectations budgétaires pour les mesures de sécurité, et il facilite le respect des lois, des ordonnances des cours, des accords de non-divulgation, des licences et d'autres obligations. C'est un moyen important d'identifier l'information qui peut être transmise en toute sécurité à un fournisseur de services d'informatique en nuage ou partagée avec les partenaires du système de justice.

POLITIQUE 2 – NOMINATION D'UN CADRE SUPÉRIEUR DE LA COUR

La cour devrait envisager de nommer ou de désigner un cadre supérieur qui a l'obligation de rendre compte à la cour et qui est responsable de mettre en oeuvre et de faire respecter la politique. Ce rôle peut être confié, par exemple, à un agent de la sécurité informatique du système judiciaire (ASISJ), à un adjoint exécutif juridique, ou au gestionnaire des documents judiciaires. Le cadre supérieur de la cour s'occupe des tâches administratives liées à la mise en oeuvre et à la gestion des politiques sur la gouvernance de l'information, y compris la classification. Il fait une mise à jour périodique du registre des actifs d'information et il procède à des examens et des vérifications pour assurer le respect de la politique. Une formation sur le traitement de l'information classifiée doit être donnée régulièrement à tous les utilisateurs.

COMMENTAIRE

Les tâches de classification confiées au cadre supérieur de la cour devraient inclure les suivantes :

1. Mettre en oeuvre et administrer la politique;
2. Communiquer les règles applicables et les meilleures pratiques à l'interne, au moyen d'interventions individuelles, de bulletins d'information, ou d'autres méthodes;

3. Établir le registre des actifs d'information (voir la politique 5) et les procédures de classification, et les mettre à jour périodiquement;
4. Former les utilisateurs et les administrateurs de système et donner des conseils à la cour sur les questions de gouvernance de l'information;
5. Vérifier la mise en oeuvre de la politique pour en assurer le respect; et
6. Contribuer aux activités d'acquisition de systèmes pour veiller à ce que les systèmes de la cour soient compatibles avec les besoins de la politique et des procédures de classification.

POLITIQUE 3 – PORTÉE

La présente politique s'applique à tous les actifs d'information judiciaire, indépendamment de l'endroit où ils se trouvent, de leur format, ou du support sur lequel ils sont transmis ou stockés.

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

Les documents personnels qui n'ont aucun rapport avec les activités de la cour sont privés et ne font pas partie des actifs d'information de la cour.

POLITIQUE 4 – TRANSITION

La présente politique (ou toute modification à celle-ci) entre en vigueur dès son approbation par la cour.

POLITIQUE 5 – REGISTRE DES ACTIFS D'INFORMATION

La cour doit créer et tenir à jour un registre des actifs d'information (RAI) qui énumère tous les actifs d'information judiciaire, en donne une brève description et les catégorise à un haut niveau.

COMMENTAIRE

Le RAI sert non seulement de base à la prise de décisions sur la classification, mais aussi de fondement à l'évaluation des menaces et des risques, à l'établissement du calendrier de

conservation de l'information judiciaire, et à l'élaboration de procédures de continuité des activités. Il s'agit de la première étape pour obtenir le contrôle de l'information judiciaire. Le RAI n'est pas un document indépendant, car il est l'élément central de l'évaluation des menaces et des risques basés sur les actifs d'information (voir la politique 6), du calendrier de conservation et des protocoles de classification. La liste est d'abord dressée, puis modifiée pour de multiples raisons, et mise à jour en conséquence. Un inventaire de haut niveau peut servir à déterminer comment l'information est créée et utilisée par la cour et par des groupes et des utilisateurs individuels. Il peut aussi aider la cour dans ses efforts pour capter le cheminement de l'information.

Les éléments descriptifs du RAI devraient être établis en fonction du volume d'information de la cour et de l'état de sa transition de l'imprimé vers le numérique. Les principaux éléments à considérer pour chaque actif d'information sont les suivants :

1. La catégorie pertinente
2. Une brève description de l'actif, y compris son objet et son usage
3. La plage de dates
4. La personne responsable de veiller à ce que l'actif soit traité et géré de manière appropriée (et ses coordonnées)
5. Le dépositaire (et ses coordonnées)
6. Les utilisateurs, y compris les relations de partage à l'interne et à l'externe
7. L'emplacement (par exemple, dans le nuage informatique, sur place, dans une base de données, dans un dépôt central)
8. Le format (par exemple, papier, numérique ou autre support)
9. Les types de demandes d'accès (y compris l'accès en bloc) qui pourraient être faites pour cet actif
10. La sensibilité de l'information (par exemple, les ordonnances de mise sous scellés, les interdictions de publication, les droits d'auteur, la protection de la vie privée, la confidentialité)

En ce qui concerne l'information numérique, il est logique d'avoir des catégories vastes et inclusives, car cette information est volumineuse, dynamique et souvent stockée dans des dépôts non structurés plutôt que dans des dossiers individuels. Plus le RAI est détaillé et précis – par exemple, une liste par titre de document – plus les actifs doivent être énumérés et suivis individuellement, ce qui alourdit le fardeau de gestion et de conformité.

Le dépositaire, le format et l'emplacement de l'information peuvent changer lorsque celle-ci circule au sein de la cour, ce qui peut compliquer la tenue de toute forme de registre. Il est donc utile d'établir des règles concernant la gestion, l'accès et l'utilisation qui s'appliquent à différents stades du cycle de vie d'un document.

Dans le RAI, les actifs d'information peuvent être répartis selon la fonction, le groupe d'utilisateurs, l'objet ou le dépôt. Par exemple, une cour peut diviser ses actifs d'information en trois grandes catégories correspondant aux concepts fondamentaux suivants :

Concept	**Catégorie**
Principe de la publicité de la justice	Dossiers judiciaires[8], documents judiciaires, plumitifs
Responsabilité partagée (magistrature et organe exécutif)	Information sur les opérations de la cour[9], documents administratifs et historiques
Indépendance judiciaire	Renseignements de la magistrature

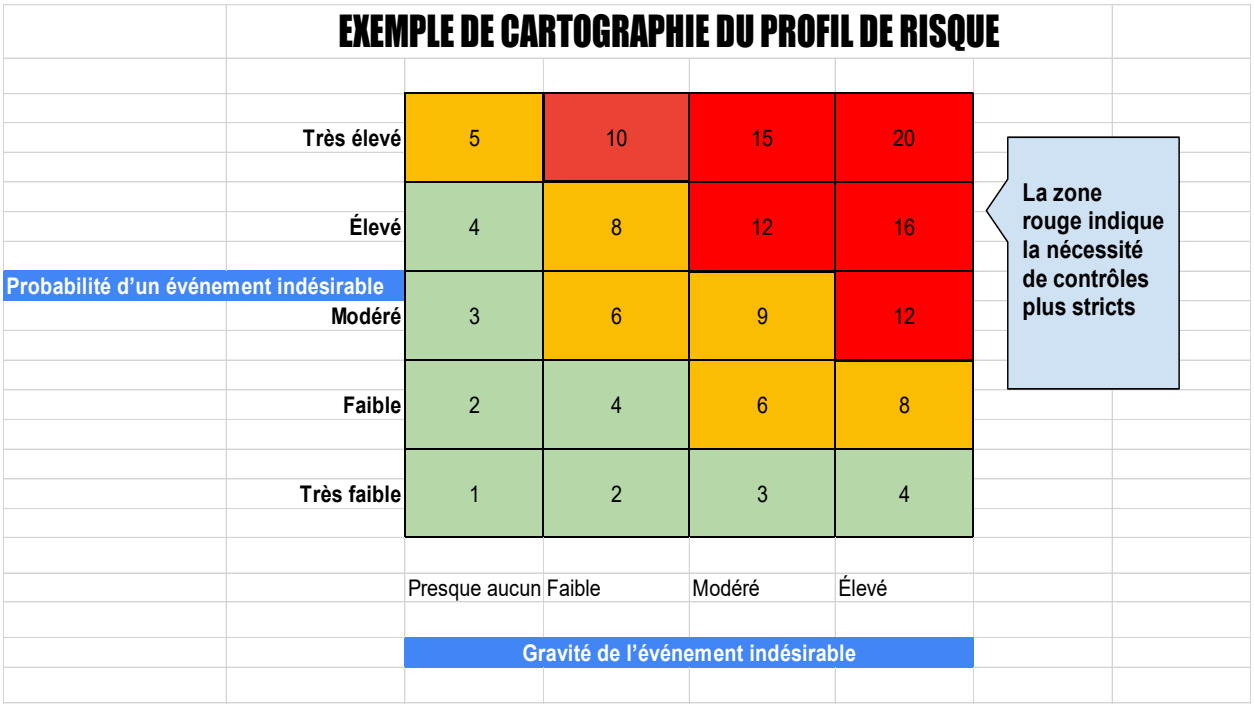
POLITIQUE 6 – ÉVALUATION DES RISQUES

La cour doit planifier et mener une évaluation des menaces et des risques (EMR), et en examiner les résultats, afin d'attribuer les niveaux de classification appropriés à chaque catégorie d'actif d'information comprise dans le RAI.[10]

[8] « Le dossier judiciaire contient 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 contenue dans les documents judiciaires et toute autre information qui a été saisie ou placée dans le dossier judiciaire. » (Définition modèle).
[9] « Information concernant la supervision, la gestion et la direction des activités nécessaires au fonctionnement de la cour ou d'autres activités assignées à l'exécutif selon la loi ou une entente (comme un protocole d'entente). » (Définition modèle)
[10] Voir la politique 3b dans le Plan directeur.

COMMENTAIRE

L'EMR aide la cour à évaluer le degré de préjudice qu'une divulgation non autorisée de l'information risquerait vraisemblablement de causer. Un graphique simplifié est présenté ci-dessous. Les risques qui y sont indiqués sont évalués par rapport à leur probabilité et à leur gravité. Ce graphique sert de base aux décideurs pour les aider à déterminer le profil de risque de la cour et à établir les contrôles de sécurité et les niveaux de classification proportionnels. Les résultats de l'EMR permettent aussi de déceler les risques résiduels qui doivent être atténués afin d'atteindre un niveau de risque acceptable pour la cour.



POLITIQUE 7 – CLASSIFICATION DES ACTIFS D'INFORMATION

Toute l'information judiciaire doit être classifiée selon la sensibilité de son contenu et les risques associés à la divulgation et à l'accès non autorisés.

Le même niveau de classification doit être attribué à toute information qui est copiée, extraite, imprimée ou autrement dérivée de l'information d'origine.

Voici les niveaux de classification à employer :

PUBLIC

S'applique à l'information qui, si elle est compromise, risquerait vraisemblablement de causer peu ou point de préjudice à une personne, à la cour ou à une autre organisation. L'information peut être rendue publique, car sa diffusion n'aurait aucun impact négatif, ou elle doit être publiée en vertu de la loi.

CONFIDENTIEL[11]

S'applique à l'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice à une personne, à la cour ou à une autre organisation.[12] L'accès interne et externe à cette information est limité aux personnes et aux organisations qui ont un besoin de savoir valable. La mention « CONFIDENTIEL » doit être apposée clairement et visiblement sur toute information de ce genre.

ACCÈS RESTREINT

S'applique à l'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice grave à une personne, à la cour ou à une autre organisation.[13] L'accès interne à cette information est limité aux personnes et aux organisations qui ont un besoin de savoir valable. L'accès externe est assujetti à une ordonnance de la cour, à la loi, à la politique de la cour, aux règles de la cour, ainsi qu'à une autorisation de sécurité et à un accord de non-divulgation approuvés par la cour. L'accès à cette information et l'usage qui en est fait doivent être consignés. L'information judiciaire d'accès restreint est assujettie à des règles plus strictes que l'information confidentielle, y compris un marquage spécial, le chiffrement et le stockage sur des supports désignés. La mention « ACCÈS RESTREINT » doit être apposée clairement et visiblement sur toute information de ce genre.

[11] Cela diffère de la suggestion faite dans le Plan directeur, dans lequel la désignation « Officiel » est proposée. Cependant, étant donné que le terme « officiel » peut servir à désigner certains types de documents judiciaires pour des raisons autres que la sécurité, il est préférable d'employer le terme « Confidentiel ».
[12] Correspond au niveau Protégé A du gouvernement canadien.
[13] Correspond au niveau Protégé B du gouvernement canadien.

SECRET

S'applique à l'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice extrêmement grave à une personne, à la cour ou à une autre organisation.[14] L'accès à cette information est limité aux personnes désignées et autorisées qui ont un besoin de savoir valable et est assujetti à un accord de non-divulgation ou à une ordonnance de la cour. L'accès à cette information et l'usage qui en est fait doivent être consignés. La mention « SECRET » doit être apposée clairement et visiblement sur toute information de ce genre. (Les marques de source originale doivent aussi être laissées en place.)

COMMENTAIRE

Chaque actif d'information judiciaire doit être classifié selon le niveau qui correspond à l'information la plus sensible dans sa catégorie. Les actifs d'information devraient être classifiés au niveau le plus faible possible, mais aussi élevé que nécessaire. Cette dynamique représente l'équilibre essentiel à atteindre entre le préjudice que pourrait causer l'accès non autorisé et les avantages de l'accessibilité de l'information pour la cour, les parties ou le public.

La classification à un niveau trop élevé peut faire augmenter les frais de maintenance, limiter l'accès légitime et encourager certains utilisateurs à contourner les contrôles de sécurité.

Des termes descriptifs tels que « Confidentiel » et « Secret » sont plus significatifs et sont donc préférables à des termes abstraits comme « Protégé A » ou « Niveau 3 ». Cependant, indépendamment des termes employés, le système de classification de l'information judiciaire proposé dans le présent modèle de politique est aligné sur les systèmes de classification des gouvernements fédéral et provinciaux du Canada, ce qui aide à réduire la confusion parmi le personnel des cours qui est appelé à utiliser à la fois l'information gouvernementale et l'information judiciaire. Pour ce qui est des tribunaux spécialisés, ils pourraient avoir besoin d'un plus grand nombre de niveaux de classification pour traiter l'information sensible qu'ils reçoivent de fournisseurs comme les gouvernements étrangers.

[14] Correspond au niveau Protégé C du gouvernement canadien.

Une façon de clarifier les différences entre les trois niveaux de classification autres que le niveau « Public » est d'expliquer aux utilisateurs que la divulgation d'information secrète causerait environ dix fois plus de dommages que la divulgation d'information d'accès restreint, et que la divulgation d'information d'accès restreint causerait environ dix fois plus de dommages que la divulgation d'information confidentielle.[15]

Les auteurs doivent savoir que l'information normalement classifiée à un faible niveau peut, dans de rares cas, nécessiter une classification de plus haut niveau. Cela s'explique par la possibilité que l'information puisse révéler un lien ou une tendance qui devrait être classifiée à un plus haut niveau que ses éléments.

POLITIQUE 8 – INFORMATION DÉJÀ CLASSIFIÉE

L'information qui a été classifiée ailleurs doit être classifiée par la cour à un niveau correspondant à celui attribué par le fournisseur et être traitée en conformité avec les contrôles de sécurité du fournisseur, dans la mesure où ceux-ci sont plus stricts que ceux de la cour.

L'information reçue d'une organisation externe doit être protégée en conformité avec toute exigence législative ou réglementaire applicable, y compris les ententes et les obligations internationales.

COMMENTAIRE

Lorsque la cour reçoit de l'information qui a été classifiée par un fournisseur, elle doit respecter les règles applicables à cette classification.

POLITIQUE 9 – DÉCLASSEMENT DE L'INFORMATION

Les contrôleurs peuvent déclasser l'information dont ils sont responsables. Les auteurs (ou leurs successeurs) peuvent déclasser leurs propres actifs d'information. Les utilisateurs ne peuvent pas déclasser un actif d'information judiciaire sans l'autorisation de son auteur ou du contrôleur.

[15] Voir Quist, *Security Classification of Information*, volume 2, chapitre 7 (en anglais seulement).

COMMENTAIRE

Les actifs d'information peuvent être classifiés à un niveau plus élevé ou plus faible, selon le besoin, avec l'autorisation nécessaire. Au fil du temps, le niveau de classification d'un document ou d'un autre actif d'information peut être modifié à la suite de l'expiration d'un délai, d'un certain événement ou d'une réévaluation de routine.

POLITIQUE 10 – MARQUAGE DE L'INFORMATION CLASSIFIÉE - BANNIÈRE

Tous les actifs d'information (y compris les copies et les imprimés) doivent être marqués d'une bannière indiquant leur niveau de classification. La bannière comprend le nom de la cour (ou son abréviation) et le niveau de classification en MAJUSCULES. En voici un exemple :

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

Au moment de la classification initiale, la bannière doit être affichée clairement et visiblement sur la face et chaque page de l'actif d'information, par exemple dans l'en-tête ou en bas de page. Si l'actif d'information ne se prête pas à un tel marquage, le niveau de classification doit être clairement associé à son sujet d'une manière adaptée à sa forme. S'il n'est pas possible d'apposer une bannière quelconque, il faut informer les utilisateurs du niveau de classification de l'actif d'information et de toute mesure spéciale concernant son traitement.

Si différentes parties d'un document n'ont pas les mêmes niveaux de classification, chaque partie devrait être marquée de façon appropriée pour indiquer son niveau de classification.

COMMENTAIRE

La bannière de classification est le principal moyen de faire connaître le degré de sensibilité d'un actif d'information. Un aspect clé à retenir est que la bannière de classification est comme un passeport, c'est-à-dire une pièce d'identité importante qui doit accompagner l'actif d'information

partout où il va. Quelle que soit la méthode employée pour apposer une bannière, elle doit être aisément visible, lisible et indélébile.

Lorsqu'un niveau de classification est prédéterminé, il peut être ajouté au modèle d'un document. Pour ce qui est des courriels, le niveau de classification devrait être indiqué dans le champ « Objet » et, facultativement, dans le texte du courriel. Le niveau de classification peut aussi être indiqué dans la signature d'un courriel, ce qui est utile lorsqu'une politique est appliquée par un utilisateur ou un groupe d'utilisateurs. De préférence, les systèmes de courriel devraient être configurés de manière à obliger les utilisateurs à choisir un niveau de classification, par exemple dans un menu déroulant, avant d'envoyer un courriel.

POLITIQUE 11 – MARQUAGE DE L'INFORMATION CLASSIFIÉE - BLOC

En plus de la bannière, les actifs d'information classifiés peuvent aussi être marqués d'un bloc de renseignements facultatif, dont l'objet est de fournir aux utilisateurs plus de détails sur l'actif d'information. Si un tel bloc de renseignements est employé, il devrait être affiché sur la face de chaque document classifié, ou d'une manière aisément visible adaptée à la forme de l'actif d'information.

Voici un exemple du contenu d'un bloc de renseignements :

Classifié par : Hon. juge en chef Moreau
Date : 2023-11-25
Raison : Preuve mise sous scellés
Déclassification : Sur ordonnance de la cour
Autres restrictions de diffusion : Aucune

COMMENTAIRE

Si le nom du responsable de la classification (le contrôleur ou l'auteur) est indiqué, les utilisateurs sauront avec qui communiquer au cas où il serait proposé de reclassifier un actif d'information. Il est utile d'indiquer la raison de la classification à des fins de vérification et de

conformité. S'il est possible d'indiquer une date de déclassification ou un fait entraînant la déclassification lorsqu'un actif d'information est créé, cela aidera les utilisateurs à prendre des décisions sur la diffusion de l'information. D'autres restrictions peuvent être utiles dans différentes circonstances, par exemple lorsqu'il s'agit de traiter des actifs d'information classifiés par des fournisseurs qui exigent plus que les contrôles minimums établis.

POLITIQUE 12 – TRAITEMENT DES ACTIFS D'INFORMATION CLASSIFIÉS

Toute l'information judiciaire doit être traitée conformément à sa classification et aux procédures énoncées dans le Guide de classification (voir l'annexe 1).

Lorsqu'une cour transmet de l'information judiciaire à un tiers, elle doit s'assurer que les politiques et procédures de sécurité du tiers sont suffisamment rigoureuses pour respecter les contrôles de classification exigés.

GLOSSAIRE

Contrôleur

Le contrôleur a le pouvoir de surveiller et de contrôler les actifs d'information. En tant que responsable de la classification, le contrôleur définit les politiques fondamentales régissant l'accès aux actifs d'information, ainsi que la classification, l'utilisation, la conservation et la disposition de ces actifs. Le contrôleur est responsable de déterminer la classification des actifs d'information judiciaire dont il a le contrôle, et il est autorisé à approuver les demandes d'accès et de déclassement. Le contrôleur doit parfois établir des contrôles de sécurité additionnels de façon ponctuelle, ou renforcer les protocoles de traitement de l'information selon les besoins.

Dépositaire

La personne ou l'entité (comme un département des technologies de l'information ou un fournisseur de services d'informatique en nuage) qui a la possession physique des actifs d'information judiciaire. Le dépositaire n'a pas le pouvoir de surveiller ou de contrôler les actifs d'information.

Actif d'information

Un ensemble de documents réunis en une unité afin de pouvoir être gérés efficacement. Le terme « actif » dans la présente politique n'est pas employé dans le sens de « propriété ».

Auteur

Un auteur est responsable de la classification des actifs d'information judiciaire qu'il produit ou reçoit d'un fournisseur. Il convient de noter que le contrôleur et l'auteur peuvent être la même personne ou la même entité. Les auteurs sont responsables de déterminer et d'appliquer les niveaux de classification aux actifs d'information qu'ils créent ou reçoivent, en conformité avec la présente politique et les directives de la cour.

Fournisseur

Une source externe qui présente ou transmet de l'information à la cour.

ANNEXE 1 : GUIDE DE CLASSIFICATION

Les tableaux suivants offrent des exemples destinés à servir de guide. Ils ne sont ni définitifs ni exhaustifs. Veuillez consulter la liste des références ci-dessous pour trouver d'autres approches ou exemples.

TABLEAU 1 : RISQUES ET ACCÈS

Classification	Niveau de risque	Description du risque	Accès
Public	Presque nul	L'information qui, si elle est compromise, risquerait vraisemblablement de causer peu ou point de préjudice à une personne, à la cour ou à une autre organisation.	L'information peut être rendue publique.
Confidentiel	Faible	L'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice à une personne, à la cour ou à une autre organisation.[16]	L'accès interne et externe à cette information est limité aux personnes et aux organisations qui ont un besoin de savoir valable.
Accès restreint	Moyen	L'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice grave à une personne, à la cour ou à une autre organisation.[17]	L'accès interne à cette information est limité aux personnes et aux organisations qui ont un besoin de savoir valable. L'accès externe est assujetti à une ordonnance de la cour, à la loi, à la politique de la cour, aux règles de la cour, ainsi qu'à une autorisation de sécurité et à un accord de non-divulgation approuvés par la cour. L'accès à cette information et l'usage qui en est fait doivent être consignés. L'information judiciaire d'accès restreint est assujettie à des règles plus strictes que l'information confidentielle, y compris un marquage spécial, le chiffrement et le stockage sur des supports désignés.

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

Classification	Niveau de risque	Description du risque	Accès
Secret	Élevé	L'information qui, si elle est compromise, risquerait vraisemblablement de causer un préjudice extrêmement grave à une personne, à la cour ou à une autre organisation.[18]	L'accès à cette information est limité aux personnes désignées et autorisées qui ont un besoin de savoir valable et est assujetti à un accord de non-divulgation ou à une ordonnance de la cour. L'accès à cette information et l'usage qui en est fait doivent être consignés.

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

TABLEAU 2 : EXEMPLES DE CONTRÔLES

Classification	En stockage	En transit	Élimination
Public	L'information peut être stockée sur des dispositifs amovibles et dans un nuage informatique public.	Aucun contrôle spécial.	Aucune exigence spéciale d'élimination.
Confidentiel	• Toutes les politiques de sécurité de base énoncées dans le Plan directeur[19] sont en place. • Sur place, l'information doit être stockée sur le réseau de la cour et protégée par des contrôles d'accès basés sur les dossiers (et sauvegardée). • L'information peut être stockée dans un nuage informatique public approuvé par la cour. • L'information peut être stockée sur des dispositifs amovibles seulement si elle est chiffrée au moyen d'outils approuvés par la cour. • Les contrôles techniques à ce niveau doivent être basés sur des produits et services sûrs et disponibles sur le marché, sans qu'il soit nécessaire de les adapter. • L'information en stockage doit être protégée par défaut. Les données doivent être transmises seulement par la voie d'un réseau sécurisé. • Les données qui passent par un réseau non fiable (non sécurisé) doivent être chiffrées selon les normes de l'industrie.	Utiliser seulement les systèmes de courriel et de textage et les autres plateformes de communication approuvés par la cour.	L'information doit être éliminée à l'aide d'outils conformes aux normes de l'industrie.
Accès restreint	• Les politiques de sécurité avancées énoncées dans le Plan directeur[20] sont en place. • L'information peut être stockée dans un nuage informatique public approuvé par la cour. • L'accès à l'information nécessite une authentification multifactorielle.	L'information doit être chiffrée au moyen d'outils approuvés par la cour.	L'information doit être éliminée à l'aide d'outils conformes aux normes de l'industrie.

[19] Les cours devraient consulter le Plan directeur pour plus de détails sur les contrôles d'accès, la sécurité physique et les autres contrôles.
[20]Les cours devraient consulter le Plan directeur pour plus de détails sur les contrôles d'accès, la sécurité physique et les autres contrôles.

Classification	En stockage	En transit	Élimination
	• L'information peut être stockée sur des dispositifs amovibles seulement si elle est chiffrée au moyen d'outils approuvés par la cour.		
Secret	• Cette information doit être protégée par les contrôles de sécurité les plus stricts qui sont raisonnablement disponibles. • Tous les accès à cette information doivent être consignés et faire l'objet d'un suivi (selon les Lignes de conduite sur la surveillance informatique[21]). • L'information ne doit pas être stockée sur des dispositifs amovibles. • L'information ne doit pas être stockée dans un nuage informatique public. • Les dépôts de données ne doivent pas être connectés à un réseau Internet public. • Les fichiers et/ou les données électroniques doivent être stockés dans un répertoire partagé de la cour ou sur un appareil fixe (c.-à-d. un ordinateur de bureau ou un serveur) et protégés par des contrôle d'accès physique et des contrôles d'accès logique basés sur les rôles. • Les fichiers et/ou les données électroniques doivent être chiffrés lorsqu'ils sont stockés sur des appareils portables ou non sécurisés. • L'information confidentielle ou sensible qui est partagée avec des tiers doit être protégée par le chiffrement des fichiers. • Les appareils portables ou non sécurisés doivent être rangés dans un endroit sûr lorsqu'ils ne sont pas utilisés.	L'information ne doit pas être transmise par courriel ni par aucun autre moyen sur des réseaux publics. L'information ne doit être partagée que par des moyens hautement sécurisés. Cela consiste notamment à utiliser des services partagés dûment autorisés et protégés par un chiffrement de haut niveau. L'information ne doit être partagée qu'avec les utilisateurs désignés.	L'information doit être éliminée de manière à être irrécupérable; il peut être nécessaire de détruire les dispositifs de stockage. Les données et les supports doivent être démagnétisés ou rendus illisibles par d'autres moyens. Il peut être nécessaire de détruire les appareils.

[21] Reproduites dans le Plan directeur.

TABLEAU 3 : MARQUAGE DE L'INFORMATION CLASSIFIÉE

Ce tableau offre quelques exemples de méthodes pour marquer l'information numérique. Quelle que soit la méthode employée, elle doit convenir au format de l'actif d'information et montrer clairement à l'utilisateur final que l'information est classifiée.

Format	Marquage
Courriel ou texto	Indiquer le niveau de classification dans le champ « Objet ». Si ce n'est pas possible, insérer la bannière au haut du texte du courriel ou du texto ou dans l'espace de signature.
Fichier texte ou image	Indiquer le niveau de classification dans les métadonnées, sur toutes les images, ou dans l'en-tête, en bas de page, ou en filigrane.
Base de données	Indiquer le niveau de classification dans l'en-tête, en bas de page ou en filigrane dans les rapports produits, ainsi que dans les métadonnées de chaque enregistrement, champ ou rapport.
Fichier audio	Insérer l'information sonore sur le niveau de classification au début du fichier.
Fichier vidéo	Insérer l'information sonore sur le niveau de classification au début du fichier. Indiquer le niveau de classification sur chaque image.

TABLEAU 4 : EXEMPLES D'INFORMATION JUDICIAIRE CLASSIFIÉE

Veuillez noter que ces listes sont tirées de plusieurs ressources publiques et internes et ne sont que des exemples. Elles ne sont ni définitives ni exhaustives. Elles montrent simplement le type d'information pouvant faire partie du cadre de politique de classification d'une cour.

Classification	Exemples
Public	• Historique de la liste des causes • Plaidoiries • Ordonnances et motifs de jugement • Transcriptions des 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 • Horaires des officiers judiciaires et calendriers des audiences • Information sur le perfectionnement professionnel • Documents concernant les réunions du personnel (autres que l'administration judiciaire) • Directives au jury • Courriels et autres communications courantes • Documents et dossiers judiciaires ne faisant pas l'objet d'une ordonnance de mise sous scellés
Accès restreint	• Projets de jugement, de décision et d'approbation • Jugements définitifs des cours s'ils font l'objet d'une interdiction de publication • Enregistrement numérique d'une procédure à huis clos • Notes de recherche, notes judiciaires • Mandats non exécutés, pardons • Ordres du jour, notes et procès-verbaux des réunions concernant l'administration judiciaire • Information sur l'administration du personnel

Classification	Exemples
	• Renseignements concernant les juges • Information obtenue par autorisation judiciaire (documents mis sous scellés, protection de l'enfance/de la jeunesse)
Secret	• Certains projets de jugement • Renseignements personnels des officiers judiciaires • Demandes de mandat de perquisition et de saisie, surveillance électronique, et documents correspondants • Information concernant les informateurs • Évaluations psychiatriques • Renseignements personnels des juges • Documents privilégiés • Information relative à la sécurité nationale