# Plan directeur pour la sécurité de l'information judiciaire

Sixième édition, avril 2021

---

Préparé par Martin Felsky, Ph.D, J.D., pour le Conseil canadien de la magistrature

## TABLE DES MATIÈRES

## INTRODUCTION À LA SIXIÈME ÉDITION

Les lecteurs remarqueront que la sixième édition du Plan directeur a un nouveau titre. Dans le passé, ce document s'appliquait à ce qu'on appelait « les renseignements judiciaires », tels que définis dans le Plan directeur et, par la suite, dans le *Cadre de politique* du Conseil canadien de la magistrature.[1] À compter de la présente édition, le Conseil confirme que les politiques du Plan directeur s'appliquent – et, en fait, se sont toujours appliquées – à la plus vaste catégorie de l'information judiciaire, telle que définie plus loin. Le rapport *Définition modèle* du Conseil explique les raisons de cet important changement de terminologie.

Ce changement répond aussi à un autre fait nouveau important survenu depuis la parution de la cinquième édition en 2018. La pandémie mondiale de la Covid-19 a sérieusement limité la capacité des cours de fonctionner efficacement en 2020 et a amené bon nombre d'entre elles à adopter des procédures en ligne peu familières ou à accélérer la mise en place de services en ligne existants. Par conséquent, ce Plan directeur traite maintenant des questions de sécurité relatives à l'utilisation de la vidéoconférence, au dépôt de documents par voie électronique et aux plateformes de collaboration.

Le Plan directeur a été rédigé sous la surveillance du Comité sur la technologie du Conseil, et en consultation avec un groupe national d'agents de la sécurité informatique du système judiciaire, à qui le Conseil est reconnaissant. Nous remercions tout particulièrement Robert Gusnowski, Agent de la sécurité informatique du système judiciaire des cours de l'Alberta, de ses suggestions détaillées, dont bon nombre ont été incorporées dans le document.

## CONTEXTE

Le Conseil canadien de la magistrature a donné suite à plusieurs recommandations qui ont été faites en novembre 2001[2] et qui reposent sur les principes fondamentaux suivants :

- Les juges et les administrateurs des cours doivent faire de la sécurité des technologies de l'information (sécurité informatique) une priorité au sein de leurs cours.

[1] Tous les renvois importants sont énumérés à l'annexe 1.

[2] Voir l'annexe 2. Le rapport complet de 2001 est confidentiel, car il traite des vulnérabilités potentielles des systèmes judiciaires.

- La sécurité informatique n'est pas seulement une préoccupation d'ordre technique; elle met aussi en cause les méthodes de planification, de gestion et d'exploitation, ainsi que les pratiques de l'utilisateur final.

- Toutes les mesures que prennent les cours en matière de sécurité informatique doivent préserver l'indépendance judiciaire ainsi que les autres aspects uniques des rapports entre les utilisateurs judiciaires et le personnel chargé de l'administration des systèmes informatiques au sein des cours, que la gestion relève du gouvernement, d'un organisme offrant des services judiciaires, ou même du secteur privé.

- La responsabilité relative aux politiques de sécurité informatique en ce qui concerne les renseignements de la magistrature est une fonction judiciaire et relève donc de la magistrature.

- La gestion, l'exploitation et les mesures techniques visant à protéger les renseignements de la magistrature conformément à la politique judiciaire sont des fonctions administratives qui relèvent, dans le cas de la plupart des cours, du gouvernement provincial.[3]

En 2013, le Conseil a adopté seize politiques fondamentales relatives à la gouvernance de l'information judiciaire, qui sont énoncées dans le *Cadre de politique*. Le *Cadre de politique* comporte aussi des politiques en matière d'accès, de protection de la vie privée, de sécurité, de préservation et de mesure du rendement. Le Plan directeur a été révisé pour le rendre conforme aux politiques applicables du *Cadre de politique*.

Le Plan directeur n'est qu'une partie de l'approche du Conseil à l'égard de la sécurité de l'information judiciaire. Pour plus de renseignements sur les initiatives connexes du Conseil, voir son site Web : www.cjc-ccm.ca.

[3] Cette question ne touche pas les cours fédérales, comme la Cour suprême du Canada, mais le gouvernement fédéral considère la prestation de services Internet (par la voie de SCNet) comme une fonction gouvernementale.

# PORTÉE ET DÉFINITIONS

## DÉFINITIONS

Les principaux termes suivants, tels que redéfinis dans le rapport *Définition modèle*, sont employés dans le Plan directeur. Les lecteurs sont encouragés à consulter ce rapport pour y trouver plus de détails et des exemples précis.

| **Terme** | **Définition** |
|---|---|
| Dossier judiciaire / *Case File* | 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. |
| Information judiciaire / *Court Information* | L'information reçue, recueillie, stockée, utilisée ou produite par une cour aux fins de sa mission. |
| Information sur les opérations de la cour / *Court Operations Information* | L'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).<br><br>Au Québec, les Outils de gestion des causes (*Case Management Tools*) et les Outils de suivi des affaires judiciaires (*Court Monitoring Tools*) sont des sous-ensembles de la vaste catégorie des Documents d'activité des tribunaux (*Court Records*) et se classent probablement le mieux sous la rubrique de l'Information sur les opérations de la cour. |
| Document judiciaire / *Court Record* | 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. Désigne l'information « officielle » sur une procédure consignée au dossier. Il s'agit de la partie du dossier judiciaire qui est accessible au public, sous réserve des restrictions relatives à la protection de la vie privée, par exemple en ce qui a trait aux renseignements personnels. |
| Information / *Information* | L'information consignée sur tout support ou sous toute forme, peu importe la manière dont elle a été créée, y compris l'information produite par des moyens humains ou autres. |

| Terme | Définition |
|---|---|
| Administration judiciaire / *Judicial Administration* | La supervision, la gestion et la direction des activités nécessaires à l'exécution des fonctions judiciaires, y compris :<br>1. la mise au rôle, la préparation, l'attribution et le jugement des affaires judiciaires;<br>2. la formation, le rendement, la conduite et la discipline des utilisatrices ou utilisateurs judiciaires;<br>3. la gouvernance de l'information judiciaire et de la technologie;<br>4. toute autre activité assignée à la magistrature selon la loi ou une entente (comme un protocole d'entente). |
| Renseignements de la magistrature[4] / *Judicial Information* | Peu importe par qui ou comment ils ont été créés, les renseignements de la magistrature comprennent :<br>1. les renseignements personnels des officières ou officiers judiciaires;<br>2. les renseignements concernant l'exercice d'une fonction judiciaire (« Renseignements décisionnels »);<br>3. les renseignements concernant l'administration judiciaire (« Renseignements administratifs »). |
| Agente ou agent judiciaire / *Judicial Agent* | Une agente ou un agent judiciaire est une utilisatrice ou un utilisateur judiciaire qui assiste une officière ou un officier judiciaire; cela peut comprendre le personnel de la cour, par exemple les cadres dirigeants, les avocats, les parajuristes, les assistants juridiques, les agents de la sécurité informatique du système judiciaire, les étudiants en droit, les stagiaires en droit, les assistants judiciaires, les adjoints administratifs, ainsi que les consultants indépendants qui travaillent sous mandat ou contrat. |
| Officière ou officier judiciaire / *Judicial Officer* | Une officière ou un officier judiciaire est une utilisatrice ou un utilisateur judiciaire qui exerce des fonctions judiciaires ou quasi judiciaires; cela comprend les juges, les juges suppléants, les conseillers-maîtres, les juges de paix, les registraires, les protonotaires ou toute personne autorisée à agir à titre de décideur. |
| Utilisatrice ou utilisateur judiciaire / *Judicial User* | Une utilisatrice ou un utilisateur judiciaire exerce des fonctions judiciaires ou y apporte son soutien, et peut être autorisé à avoir accès aux renseignements de la magistrature à différents niveaux d'habilitation, selon son rôle. |

[4] « *Judicial Information* » a été traduit dans le passé par « Information judiciaire ». Cependant, pour éviter la confusion, « *Judicial Information* » devrait être traduit par « Renseignements de la magistrature ».

## MAGISTRATURE

Le terme « magistrature » est employé tout au long du Plan directeur. Dans toute politique, « la magistrature » peut désigner l'effectif des juges d'une cour particulière, le cabinet du juge en chef d'une cour, un représentant désigné du juge en chef, ou un comité de juges responsable de la technologie au sein d'une juridiction.

## PORTÉE

Bien que le mandat légal du Conseil ne vise que les juges de nomination fédérale, il arrive souvent que ces juges partagent des plateformes et des ressources technologiques avec leurs collègues de nomination provinciale. Pour cette raison, entre autres, la collaboration est encouragée en ce qui a trait à l'élaboration des politiques en matière de sécurité. Le Plan directeur s'applique à tout système informatique utilisé pour obtenir accès à l'information judiciaire. Cela comprendrait les services d'informatique en nuage, les ordinateurs domestiques, les supports d'information amovibles, les réseaux de transmission de données et les appareils mobiles.

La sécurité des systèmes informatiques est un domaine complexe, et la portée du Plan directeur ne se veut pas générale ni technique. De plus, le Conseil s'intéresse principalement au rôle de la magistrature dans l'élaboration des politiques et des normes, et non pas aux détails de la gestion d'un service des technologies. À cet égard, le Plan directeur ne couvre pas chacun des aspects de l'administration de la sécurité. Il ne traite pas non plus de la sécurité de l'information qui n'est pas sous forme numérique, de la sécurité des communications par téléphone ou télécopieur, ni de la sécurité physique des palais de justice et de leurs occupants.

Le Plan directeur vise à adapter et à améliorer les politiques et programmes existants des gouvernements et des administrations des cours. Dans cette mesure, le Plan directeur est basé sur les normes, lignes directrices, contrôles et pratiques exemplaires réputés à l'échelle mondiale en matière de sécurité de l'information, dont certains sont énumérés plus loin dans la section intitulée Principaux renvois, et il est conçu pour être utilisé conjointement avec ceux-ci.

## RÉSUMÉ DES PRINCIPAUX CHANGEMENTS DANS LA SIXIÈME ÉDITION

1. Le titre a été changé pour refléter la portée réelle de l'élaboration des politiques judiciaires et pour normaliser les versions française et anglaise.
2. De nouvelles politiques concernant le travail à distance, les audiences virtuelles et les plateformes de collaboration ont été ajoutées.
3. Les définitions des principaux termes ont été modifiées et mises à jour.
4. L'ordre des politiques a été changé afin d'assurer une suite plus logique.
5. Les renvois et les liens hypertextes ont été mis à jour.
6. L'annexe 3 (Exemple de politique de sécurité des appareils mobiles) a été supprimée.
7. Le glossaire a été élargi et mis à jour.

# POLITIQUES

## 1. INDÉPENDANCE JUDICIAIRE

**Politique 1a :** Toutes les mesures que prennent les cours en matière de sécurité de l'information doivent préserver l'indépendance judiciaire ainsi que les autres aspects uniques des rapports entre les *utilisateurs judiciaires* et le personnel chargé de l'administration des cours, que la gestion relève du gouvernement, d'un organisme de services judiciaires ou du secteur privé.

**Politique 1b :** Les *utilisateurs judiciaires* doivent disposer de leur propre domaine de sécurité, qu'il soit isolé par séparation physique ou logique, ou par une combinaison des deux. L'architecture du réseau, la configuration, les contrôles d'accès et le soutien opérationnel doivent au minimum être conformes à la plus récente édition du Plan directeur.

**Politique 1c** : Peu importe qui en a la garde ou qui y a accès, les *renseignements de la magistrature* appartiennent toujours à celle-ci.

**Commentaire :**

L'indépendance judiciaire est un principe constitutionnel fondamental. Elle s'applique, dans l'intérêt du public, à la magistrature en général ainsi qu'à chaque juge individuel. L'indépendance judiciaire comprend la protection contre toute influence abusive, mais surtout l'indépendance vis-à-vis de l'organe exécutif du gouvernement, qui plaide souvent devant les cours. L'un des éléments clés de l'indépendance judiciaire est l'indépendance administrative, à laquelle la gouvernance et l'application des technologies de l'information sont étroitement liées.[5] Étant donné qu'une magistrature indépendante suscite la confiance du public dans le système de justice, l'*apparence* d'indépendance doit également être soigneusement préservée.

**Renvoi :** NIST SP-800-171r2.

**Cadre de politique :** Tous les juges et tout le personnel des cours devraient utiliser un domaine Internet

[5] [traduction] « Notre Constitution exige que les juges à tous les niveaux bénéficient de l'inamovibilité, de la sécurité financière, de l'indépendance administrative et de l'autonomie décisionnelle. » Hon. Ian Binnie, « *Judicial Independence in Canada* », http://www.venice.coe.int/WCCJ/Rio/Papers/CAN_Binnie_E.pdf, page 34. (consulté le 21 janvier 2021)

commun qui est séparé de celui du gouvernement et ils devraient employer ce domaine pour toutes leurs communications. (Politique fondamentale n° 8)

## 2. SURVEILLANCE

**Politique 2a** : Toute surveillance des *utilisateurs judiciaires* doit se faire en conformité avec les *Lignes de conduite sur la surveillance informatique* (2002) du Conseil canadien de la magistrature : « Il est primordial de bien définir et d'être en mesure de justifier le but de la surveillance informatique des juges et du personnel judiciaire qui relève directement des juges. La surveillance informatique doit respecter le caractère secret des délibérations, la confidentialité, le droit à la protection de la vie privée et l'indépendance de la magistrature. »

**Politique 2b** : Les outils analytiques (y compris ceux qui font usage de l'intelligence artificielle) ne peuvent être appliqués à l'*information judiciaire*, que celle-ci soit anonymisée ou non, sans l'avis et l'approbation de la magistrature.

**Commentaire** :

Alors que la surveillance du contenu – comme l'enregistrement des frappes, l'examen de l'historique de navigation sur le Web, et la recherche automatisée par mot-clé dans les courriels – constituerait une violation directe de la vie privée des juges, y compris le caractère secret des délibérations, toute forme de surveillance peut potentiellement compromettre l'indépendance judiciaire. Par exemple, les journaux d'événements peuvent contenir des données sensibles et des renseignements permettant d'identifier une personne. La recherche judiciaire peut nécessiter l'accès à des sites Web qui sont systématiquement interdits aux utilisateurs non judiciaires.

**Renvois** : NIST SP800-53r5, ISO 27001:2013 18.1.4 et ISO 29100.

**Cadre de politique :** Une évaluation des facteurs relatifs à la vie privée doit avoir lieu au stade de conception des systèmes de gestion de l'information judiciaire qui pourraient servir à recueillir, à récupérer, à utiliser ou à diffuser des renseignements personnels. (Politique de protection de la vie privée n° 3)

## 3. POLITIQUE

**Politique 3a :** La responsabilité des politiques relatives à l'*information judiciaire*, y compris la sécurité de l'information, est une fonction judiciaire qui, de ce fait, relève de la magistrature. La gestion, les opérations et les mesures techniques visant à protéger l'*information judiciaire* conformément aux politiques judiciaires sont des fonctions administratives qui relèvent, dans la plupart des cours, d'un organisme gouvernemental.

**Politique 3b :** Chaque cour doit planifier et mener chaque année une évaluation des menaces et des risques (« EMR ») en collaboration avec la magistrature. Le degré de détail nécessaire et la portée d'une EMR peuvent varier d'une cour à une autre, selon les circonstances.

**Renvois :** NIST SP800-53r5, 12-PL, 14-RA, ISO 27001:2013, A.5. Voir la norme ISO/IEC 27005 pour des conseils sur la gestion des risques.

**Cadre de politique :** Les politiques de gestion de l'information seront publiées sur le site Web de la cour. (Politique d'accès n° 7)

## 4. GOUVERNANCE

**Politique 4 :** La sécurité de l'*information judiciaire* doit être gérée dans le cadre d'un programme de sécurité formel et documenté qui est autorisé et adéquatement financé par l'organisme gouvernemental responsable de l'administration des cours. L'administration des cours doit décrire dans un plan écrit la manière dont les exigences de la magistrature en matière de sécurité doivent être remplies.

**Commentaire :**

La sécurité de l'*information judiciaire* ne peut être laissée à des processus *ad hoc*, informels et non documentés, et sa responsabilité ultime ne peut être déléguée à des employés subalternes. Des budgets adéquats doivent être alloués afin d'assurer la sécurité et l'intégrité de l'*information judiciaire*, conformément à l'évaluation des menaces et des risques.

**Renvois :** ISO 27001:2013, A.6.

## 5. AGENT DE LA SÉCURITÉ INFORMATIQUE DU SYSTÈME JUDICIAIRE

**Politique 5 :** Chaque juridiction doit veiller à ce qu'un *Agent de la sécurité informatique du système judiciaire* (ASISJ) qui est responsable envers la magistrature soit nommé pour surveiller la gestion des mesures de sécurité informatique de l'*information judiciaire*.

Le rôle principal de l'ASISJ consiste à conseiller la magistrature dans ses négociations et son étroite coopération avec l'administration des cours et les fournisseurs tiers à l'égard des questions relatives à la sécurité de l'information. L'élément clé est que l'ASISJ doit être fonctionnellement responsable envers la magistrature seulement, afin d'éviter tout conflit d'intérêts potentiel. Dans certaines juridictions, l'ASISJ peut faire partie d'une organisation qui offre un soutien aux utilisateurs judiciaires; les qualifications, les rôles et les responsabilités spécifiques d'une équipe d'ASISJ doivent être déterminés en fonction des besoins de chaque cour.

## 6. SENSIBILISATION ET FORMATION

**Politique 6 :** Une formation adéquate sur la protection des renseignements personnels et la sensibilisation à la sécurité doit être donnée à tous les utilisateurs du système, y compris les *utilisateurs judiciaires*, et une formation plus avancée relative au rôle doit être donnée à tout utilisateur qui a accès à l'*information judiciaire*.

**Commentaire :**

Les utilisateurs finals qui ne sont pas suffisamment formés représentent un danger réel pour toute organisation. La sensibilisation, la formation et l'éducation en matière de sécurité sont nécessaires pour assurer le succès de tout programme de sécurité de l'information. Le programme de formation doit comprendre de la documentation sur l'indépendance de la magistrature et la situation constitutionnelle particulière des *utilisateurs judiciaires*.

**Renvois :** NIST SP800-53r5, 3-AT, ISO 27002:2013, 7.2.2.

## 7. SÉCURITÉ PHYSIQUE

**Politique 7 :** Toutes les installations et tout l'équipement servant au traitement de l'*information judiciaire* doivent être situés dans un lieu sécurisé, dont l'accès est limité aux personnes autorisées. Les mesures de sécurité physique doivent être conçues pour protéger l'*information judiciaire* contre les catastrophes naturelles ou les menaces humaines, conformément à l'évaluation des menaces et des risques.

**Commentaire :**

La sécurité physique désigne la protection des sites et de l'équipement (et de l'information et des logiciels qu'ils contiennent) contre l'introduction par effraction, le vol, le vandalisme, les catastrophes naturelles ou autres, et les dommages accidentels. Les gestionnaires doivent se préoccuper de la construction des centres de données, de la répartition des salles, des procédures d'urgence, des règlements régissant la disposition et l'utilisation de l'équipement, de l'alimentation en énergie et en eau, de la manutention des produits, ainsi que des relations avec le personnel, les entrepreneurs externes, les autres cours, les ministères, les organismes gouvernementaux et les tribunaux. Ces mesures s'appliquent peu importe que l'équipement se trouve sur place ou non, et elles comprennent la sécurité physique des actifs servant à obtenir accès à l'*information judiciaire* à distance.

**Renvois :** NIST SP800-53r5, 11-PE, ISO 27001:2013, A.11.

## 8. SYSTÈMES D'INFORMATION

**Politique 8 :** Les processus d'acquisition, de développement et de maintenance des systèmes d'*information judiciaire* doivent être conçus et appliqués de manière à préserver la qualité, l'intégrité et la disponibilité à long terme de l'information judiciaire. Les renseignements de la magistrature exigent une protection additionnelle en plus des mesures de sécurité appliquées à l'*information judiciaire* plus généralement.

**Commentaire :**

En plus du piratage informatique de faible niveau, des tentatives de connexion au hasard et du piratage psychologique, les administrateurs des cours devraient être attentifs aux risques associés aux menaces persistantes avancées.

**Renvois :** ISO 27001:2013, A.14, NIST SP800-53r5, 15-CA, 18-SA.

**Cadre de politique :** Politique fondamentale n° 10, Politique de sécurité n° 5.

## 9. COMMUNICATIONS ET OPÉRATIONS

**Politique 9a :** Les programmes de sécurité de la cour doivent comprendre des contrôles, des procédures et des pratiques opérationnels documentés et approuvés, ainsi que des responsabilités bien définies. Des politiques, procédures et contrôles formels additionnels doivent être utilisés afin de protéger l'échange et la publication de l'*information judiciaire* par n'importe quel type de moyen de communication ou de technologie.

**Politique 9b :** Les cours ont la responsabilité de mettre en place les contrôles nécessaires pour se protéger contre les codes malveillants, les attaques par déni de service et les menaces externes similaires.

**Commentaire :**

Les éléments clés de la sécurité opérationnelle définis dans la norme ISO 27001:2013 sont les suivants :

1. Procédures d'exploitation documentées
2. Gestion des changements
3. Gestion de la capacité
4. Séparation des environnements de développement, de test et d'exploitation
5. Protection contre les logiciels malveillants
6. Sauvegarde
7. Journalisation et surveillance
8. Synchronisation des horloges
9. Maîtrise des logiciels d'exploitation
10. Installation de logiciels sur des systèmes d'exploitation
11. Gestion des vulnérabilités techniques
12. Restrictions liées à l'installation de logiciels
13. Mesures de vérification des systèmes d'information

**Renvois :** ISO 27001:2013, A.12, A.13, NIST SP800-53r5, 16-SC.

**Cadre de politique :** Les cours doivent adopter et tenir à jour des pratiques exemplaires pour protéger les réseaux locaux sans fil et veiller à ce que les *utilisateurs judiciaires* ne compromettent pas la sécurité de l'*information judiciaire* lorsqu'ils utilisent ces réseaux. (« Si un point d'accès public sans fil à Internet est installé dans un palais de justice, il ne doit pas compromettre l'*information judiciaire*. » Politique de sécurité n° 6)

Les systèmes et les technologies d'*information judiciaire* des cours devraient être obtenus, conçus et mis en œuvre de manière à faciliter l'interopérabilité et l'échange de données entre différents systèmes, sans compromettre l'indépendance des systèmes, l'indépendance judiciaire ni le rôle des cours comme dépositaires des *dossiers de la cour*. (Politique fondamentale n° 4)

## 10. GESTION ET SIGNALEMENT DES INCIDENTS

**Politique 10 :** Chaque cour doit mettre en place un protocole pour le signalement des incidents de sécurité ayant trait aux *utilisateurs judiciaires* et aux *renseignements de la magistrature*, afin d'assurer le respect des principes de l'indépendance judiciaire. Les incidents touchant la sécurité de l'information doivent être signalés promptement et uniquement selon la voie hiérarchique approuvée.

**Commentaire :**

Toute personne ayant des motifs de croire que la sécurité est menacée ou qu'il y a eu atteinte à la sécurité doit prendre des mesures pour signaler l'incident promptement à la ou aux personnes appropriées. Pour les besoins du processus de signalement des incidents, tous les employés doivent être sensibilisés et recevoir une formation sur les mesures de sécurité, les signes avant-coureurs d'une atteinte à la sécurité, et les mécanismes de signalement appropriés.

Les différents types d'atteintes à la sécurité comprennent la diffusion publique de documents judiciaires faisant l'objet d'un interdit de publication, ainsi que la publication de documents judiciaires avant qu'elle ne soit autorisée par la cour.

Les *Lignes de conduite sur la surveillance informatique* prévoient que : « Toute surveillance informatique devrait être administrée par le personnel qui relève directement du juge en chef de la cour et qui est responsable seulement devant ce dernier. » Ce principe devrait s'appliquer également au signalement d'incidents impliquant les *utilisateurs judiciaires*.

**Renvois :** NIST SP800-53r5, 7-IR. ISO 27001:2013, A.16.

## 11. CONTINUITÉ DES ACTIVITÉS

**Politique 11 :** Les cours doivent protéger l'*information judiciaire* en cas de catastrophe, pandémie ou autres défaillances du système, et fournir un degré élevé d'assurance que toute perturbation du service résultant d'un tel événement sera aussi bref que possible. Les *utilisateurs judiciaires* doivent avoir accès au stockage de données, et les données stockées doivent être sauvegardées de manière sécuritaire au moins une fois par jour. Des mesures efficaces doivent être prises pour faciliter la sauvegarde de l'*information judiciaire* qui est créée ou reçue (si elle est stockée localement), par exemple sur des appareils mobiles.

**Commentaire :**

Un plan de continuité des activités doit être préparé en se basant sur l'évaluation des menaces et des risques, et ce plan devrait inclure un processus de mise à jour. Tous les plans de continuité des activités doivent être conformes au Plan directeur et comprendre au moins les éléments suivants :[6]

1. Gouvernance
2. Analyse des répercussions sur les activités
3. Plans, mesures et dispositions pour la continuité des activités
4. Procédures, essais et formation en matière de préparation
5. Techniques d'assurance de la qualité (exercices, entretien régulier et vérification)

**Renvois :** NIST SP800-53r5, 5-CP; ISO 27001:2013, A.17.

[6] Pour plus de renseignements, voir Gouvernement du Canada, Planification de la continuité des activités, (consulté le 21 janvier 2021)

## 12. SÉCURITÉ DU PERSONNEL

**Politique 12a :** Toutes les cours doivent avoir des procédures documentées pour l'orientation et les départs, et elles doivent offrir une formation continue aux employés et aux entrepreneurs qui ont accès à l'*information judiciaire*. Des processus doivent être en place pour s'assurer que les employés et les entrepreneurs aient le niveau d'autorisation de sécurité approprié. Les procédures doivent prévoir des mesures disciplinaires en cas d'infraction aux politiques sur la sécurité de l'*information judiciaire*. Des procédures doivent être en place pour assurer le retrait de l'accès à l'*information judiciaire* d'un employé ou d'un entrepreneur lorsqu'il quitte ou qu'il change de rôle.

**Politique 12b :** Les utilisateurs qui ont accès à l*'information judiciaire* doivent obtenir seulement les autorisations minimales nécessaires à l'exercice de leurs fonctions, en conformité avec le principe du « droit d'accès minimal ».

**Politique 12c :** Une personne ne peut obtenir accès à l'*information judiciaire* à moins de satisfaire aux exigences de la présente *politique* et d'avoir obtenu le niveau d'autorisation de sécurité gouvernementale correspondant à son rôle.

**Commentaire :**

Avant d'obtenir un accès à de l'*information judiciaire*, un utilisateur doit satisfaire au minimum aux exigences suivantes :

1. besoin de savoir;
2. avoir fait l'objet d'une vérification des antécédents par la police;
3. avoir satisfait aux autres procédures applicables en matière de filtrage de sécurité;
4. avoir été informé de la nature particulière de l'*information judiciaire* (« Des stratégies de formation du personnel doivent être adoptées afin de mieux faire comprendre le caractère délicat de l'*information judiciaire* », Cadre de politique, Politique de sécurité n° 4);

5. avoir reçu une formation sur toutes les politiques, procédures et pratiques de sécurité applicables;

6. avoir signé une entente énonçant ses obligations en matière de sécurité de l'*information judiciaire.*

**Renvois :** NIST SP800-53r5, 10-PS, ISO 27001:2013, A.7

**Cadre de politique :** Les contrats d'engagement du personnel, des consultants et des entrepreneurs doivent contenir des ententes de confidentialité pour prévenir la divulgation d'*information judiciaire* confidentielle. (Politique de sécurité n° 2)

## 13. CONTRÔLE D'ACCÈS

**Politique 13a :** En ce qui concerne l'*information judiciaire*, la magistrature est responsable de toutes les décisions de contrôle d'accès. Les utilisateurs devraient obtenir le niveau minimal d'accès nécessaire à leur rôle et correspondant à leur niveau d'autorisation de sécurité. L'accès à l'administration du système ne devrait être accordé aux *utilisateurs non judiciaires* que de façon extrêmement limitée et uniquement pour leur permettre de fournir un soutien administratif. Un tel accès à des *utilisateurs non judiciaires* ne devrait leur être accordé que sur demande, puis leur être retiré une fois que la raison d'être immédiate de l'accès a été accomplie.

**Politique 13b :** Les systèmes d'*information judiciaire* qui contiennent des *renseignements de la magistrature* doivent être gardés dans un lieu adéquatement protégé et, si possible, faire l'objet d'une surveillance accrue, comporter des contrôles d'accès rigoureux et être protégés par le cryptage. Les cours doivent prendre des mesures suffisantes pour enregistrer les opérations effectuées dans tous les serveurs et dispositifs du réseau, afin de pouvoir déceler les tentatives d'accès non autorisé et les séquences d'opérations suspectes. Toute activité de ce genre de la part des *utilisateurs judiciaires* est assujettie en tout temps aux *Lignes de conduite sur la surveillance informatique* et doit être portée à l'attention de la magistrature.

## Commentaire :

Cette politique ne suppose pas que la magistrature a le pouvoir exclusif de déterminer les rôles et les niveaux d'autorisation de sécurité; l'administration des cours doit aussi avoir le pouvoir de déterminer les niveaux d'accès appropriés des utilisateurs, car le personnel des cours peut avoir de doubles responsabilités en matière de reddition de comptes. Selon les principes généraux énoncés dans le *Cadre de politique*, cependant, l'administration des cours ne peut donner à un utilisateur un niveau d'accès plus élevé que celui accordé par la magistrature.

**Renvois :** NIST SP800-53r5, 1-AC, ISO 27001:2013, A.9.

**Cadre de politique :** L'*accès en bloc* à une partie ou à l'ensemble des *dossiers de la cour* doit être régi par une entente écrite conclue avec la cour et portant sur les principales questions et les principaux risques. (Politique d'accès n° 5).

L'*information judiciaire* doit être protégée contre l'accès non autorisé en conformité avec le Plan directeur du Conseil canadien de la magistrature pour la sécurité de l'*information judiciaire*. (Politique de sécurité n° 1).

Les listes de contrôle doivent être surveillées de près afin de pouvoir identifier facilement les utilisateurs qui ont accès à l'information judiciaire à n'importe quel moment. (Politique de sécurité n° 3).

## 14. TÉLÉTRAVAIL ET ACCÈS À DISTANCE AUX SYSTÈMES

**Politique 14a :** Les cours doivent établir et documenter des bases de référence concernant les restrictions d'utilisation, la configuration des systèmes, les exigences de connexion, et les modes d'application pour chaque type d'accès à distance permis.

**Politique 14b :** En consultation avec la magistrature, les cours doivent établir des modalités et conditions précises concernant l'usage de systèmes externes, qui sont conformes aux politiques et procédures de sécurité de la cour et qui spécifient la plus haute catégorie de sécurité de l'information pouvant être traitée, stockée ou transmise par la voie de systèmes externes. Les *utilisateurs judiciaires* à distance devraient disposer de ressources adéquates pour répondre aux exigences de la Cour en matière de sécurité.

**Commentaire :**

Le télétravail représente maintenant un concept plus large que l'accès à distance. La sécurité de l'accès à distance n'est pas seulement l'affaire des responsables des technologies de l'information – elle a aussi de l'importance pour les personnes qui travaillent à domicile ou ailleurs, surtout de façon régulière. De plus, les utilisateurs – qu'ils se trouvent au palais de justice ou ailleurs – utilisent de plus en plus des plateformes et des systèmes externes (en d'autres mots, des services logiciels qui ne sont pas gérés par l'administration de la cour). Des pratiques exemplaires devraient être établies et faire partie d'un programme de formation obligatoire, qui devrait comprendre des sujets tels que la sécurité physique.

**Renvois :** *Accès à distance* : NIST AC-17, *Utilisation de systèmes externes* : NIST AC-20, *Conseils de sécurité pour les organisations dont les employés travaillent à distance* (ITSAP.10.016),[7] *National Security Agency, Selecting and Safely Using Collaboration Services for Telework – UPDATE*.[8]

[7] Centre canadien pour la cybersécurité, https://cyber.gc.ca/fr/orientation/problemes-de-securite-lies-au-teletravail-itsap10016. (consulté le 21 janvier 2021)
[8] https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/Collaboration_Services_UOO13459820_Full.PDF. (consulté le 21 janvier 2021)

## 15. GESTION DES APPAREILS MOBILES

**Politique 15 :** Les cours doivent établir une politique conforme au Plan directeur pour les appareils mobiles et mettre en place des outils et des protocoles de sécurité permettant d'effacer les données des appareils perdus ou volés.

**Commentaire :**

Qu'ils soient fournis par l'administration de la cour, utilisés dans le cadre d'une politique officielle sur l'usage d'appareils personnels, ou utilisés entièrement en dehors du programme de sécurité de la cour, les appareils mobiles posent un défi aux approches traditionnelles en matière de sécurité de l'information.

Les appareils mobiles, qu'ils soient fournis par la cour ou, comme on le voit de plus en plus, achetés par les utilisateurs eux-mêmes, présentent de nombreux risques pour la sécurité.

1. Premièrement, les appareils mobiles peuvent être configurés pour accéder facilement et de partout aux ressources d'information en réseau. Cependant, contrairement aux ordinateurs de bureau ou aux ordinateurs portables, qui sont obtenus, fournis, configurés et entretenus par l'administration de la cour, les appareils mobiles ne sont généralement pas conçus, ni construits ou configurés avec les mêmes capacités de sécurité en tête.

2. Deuxièmement, les appareils mobiles sont des ordinateurs qui peuvent générer, traiter et stocker des données. Cependant, selon leur configuration, la protection par mot de passe de ces appareils peut être faible, les options de chiffrement peuvent être limitées ou inexistantes, et les appareils peuvent être facilement égarés ou volés, ce qui peut causer de graves atteintes à la sécurité et à la vie privée.

3. Troisièmement, la popularité des applications gratuites et peu coûteuses est largement responsable de la montée en popularité des appareils mobiles. L'utilisation de ces applications est extrêmement commode, mais elle présente de multiples risques, car les données créées par l'utilisateur et ses données personnelles sont transmises – souvent à son insu – aux tiers qui créent les applications.

4. Quatrièmement, les appareils mobiles sont toujours connectés à Internet, et les capacités GPS qui y sont intégrées permettent de suivre en temps réel la position et les activités de l'utilisateur. Si l'appareil est compromis, la caméra et le microphone intégrés peuvent aussi être utilisés pour enregistrer et transmettre des événements et des conversations sans que l'utilisateur ne le sache.

## 16. CLASSIFICATION DE L'INFORMATION JUDICIAIRE

**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.

**Commentaire :**

L'auteur d'un document devrait être responsable d'attribuer le niveau de classification approprié à l'information qu'il a créée. Les documents autorisés à être accessibles au public peuvent être déclassifiés (ou, le cas échéant, non classifiés dès le départ). Toute personne qui travaille avec la cour a le devoir de respecter la confidentialité et l'intégrité de l'information et des données judiciaires auxquelles elle a accès, et elle est personnellement responsable de protéger les actifs en conformité avec la présente politique.

Le système suivant de classification à trois niveaux est un modèle que les cours peuvent utiliser. D'autres méthodes peuvent être adoptées pour répondre aux besoins locaux, bien que l'uniformité parmi l'ensemble des cours serait préférable. Les administrateurs des cours peuvent exiger des contrôles plus rigoureux pour gérer les risques à la sécurité et à la vie privée auxquels sont exposées les données agrégées, ou pour gérer les préoccupations en matière d'intégrité et de disponibilité.

**Cour - Officiel** – La majeure partie de l'*information judiciaire* est classifiée par défaut comme étant « officielle », et elle est donc assujettie aux mesures de protection énoncées dans le Plan directeur. Cela comprend les activités et les services administratifs courants, dont certains pourraient avoir des conséquences dommageables en cas de perte, de vol ou de diffusion dans les médias, sans toutefois être exposés à un niveau de menace élevé. Il n'est pas nécessaire que l'information courante porte explicitement la mention « Cour - Officiel ».

**Cour - Accès restreint** – Ce niveau de classification est utilisé pour l'*information judiciaire* sensible, par exemple : les documents qui contiennent des renseignements personnels concernant un juge, une affaire ou une partie, les projets de jugement, les courriels concernant un avis juridique ou la jurisprudence, ainsi que les notes de service portant sur des questions concernant la magistrature. L'*information judiciaire* d'accès restreint est assujettie à des règles plus strictes que l'*information judiciaire* officielle, notamment un marquage spécial, le chiffrement et le stockage sur des supports désignés. La mention « COUR - ACCÈS RESTREINT » doit être apposée clairement et visiblement sur toute information de ce genre.

**Cour - Secret** – Ce niveau de classification est utilisé pour l'*information judiciaire* la plus sensible, y compris, par exemple, les renseignements gouvernementaux, les dossiers judiciaires sous scellé, ainsi que les rapports de police qui exigent le plus haut niveau de protection contre les plus graves menaces. Les marques de source originale doivent aussi être laissées en place. La mention « COUR - SECRET » doit être apposée clairement et visiblement sur toute information de ce genre.

L'auteur est responsable de classifier et de marquer l'information, et peut aussi décider de changer le niveau de classification ou de déclassifier l'information selon le besoin.

Les documents peuvent être classifiés à un niveau plus élevé ou plus bas, ou être déclassifiés, avec l'autorisation nécessaire. Par exemple, lorsqu'un projet de jugement (portant la mention « COUR - ACCÈS RESTREINT ») est finalisé et prêt à être rendu public selon les instructions

du juge, il y a lieu d'y apposer la mention « COUR - DÉCLASSIFIÉ » et d'indiquer la date de déclassification. Au fil du temps, le niveau de classification d'un document ou d'autres actifs peut être modifié à la suite de l'expiration d'un délai ou d'une réévaluation courante.

En ce qui concerne les actifs d'information, les points suivants doivent être pris en compte[9] :

1. L'emploi d'un niveau de classification trop élevé peut entraver le partage de l'information et mener à la prise de mesures de contrôle inutiles et coûteuses; l'emploi d'un niveau de classification trop faible peut mener à la prise de mesures de contrôle insuffisantes et exposer les actifs d'information sensibles à un plus grand risque de compromission.

2. Dans un document, le niveau de classification doit être indiqué en MAJUSCULES au haut et au bas de chaque page. L'information plus sensible devrait être séparée et mise en annexe, afin que le corps du document puisse être distribué à plus grande échelle.

3. Le niveau de classification des documents sensibles partagés à l'interne doit aussi être clairement indiqué.

4. Il est recommandé d'indiquer le niveau de classification dans l'objet et/ou le texte d'un courriel. Lorsque cela est possible, le système devrait obliger les utilisateurs à choisir un niveau de classification, par exemple dans un menu déroulant, avant que le courriel ne puisse être envoyé.

5. Un dossier ou un groupe de documents ou d'actifs d'information sensibles doivent être classifiés selon le niveau de classification le plus élevé de l'information qui s'y trouve. Par exemple, un dossier imprimé ou un échange de courriels qui contient à la fois de l'information désignée « COUR - OFFICIEL » et « COUR - SECRET » doit être classifié au niveau plus élevé (c.-à-d. « COUR - SECRET »).

6. Les courriels sont souvent des documents de conversation auxquels plusieurs personnes ajoutent de l'information en réponse à une requête ou une question. Les destinataires

[9] Tiré de *UK Cabinet Office*, *Government Security Classifications*, mai 2018 version 1.1.

individuels doivent évaluer tout le contenu d'un échange de courriels avant d'y répondre ou de le faire suivre.

7. Dans certaines circonstances, il peut y avoir une bonne raison de partager à plus grande échelle certains éléments d'information d'un rapport sensible. En prévision d'un tel besoin, les auteurs du rapport devraient examiner la possibilité de produire un sommaire épuré ou d'employer une formulation préalablement convenue dont le niveau de classification est plus bas.

**Renvois :** Gestion des actifs ISO 27001:2013, A.8, *UK Cabinet Office*, *Government Security Classifications*, mai 2018 version 1.1.

## 17. CRYPTAGE ET SIGNATURES

**Politique 17a :** La magistrature doit participer à l'élaboration de la politique de cryptage et à sa mise en application, en ce qui concerne la confidentialité, l'intégrité, la non-répudiation et l'authentification de l'*information judiciaire*. La politique et les procédures de *cryptage* doivent être conformes au système de classification de l'*information judiciaire*. Les activités principales de gestion, y compris les politiques et les procédures, doivent relever de la magistrature.

**Politique 17b :** Afin d'assurer la pleine indépendance, il est recommandé que l'autorité de certification des *utilisateurs judiciaires* soit un tiers de confiance indépendant du gouvernement.

**Politique 17c :** La décision de crypter des données devrait être fondée sur des décisions documentées de gestion des risques à la sécurité de la cour et sur l'application du système de classification de l'*information judiciaire*.

**Politique 17d :** Les cours devraient fournir aux *utilisateurs judiciaires* autorisés des signatures numériques ou électroniques sécurisées afin de faciliter le déroulement sûr des activités dans un environnement judiciaire virtuel.

**Commentaire :**

L'objectif de cette politique est de rendre les outils de chiffrement facilement accessibles aux *utilisateurs judiciaires*, de gérer le processus de *cryptage* de façon sécuritaire, de veiller à

préserver l'indépendance judiciaire, et de protéger l'information sensible contre tout accès non autorisé. L'usage de signatures numériques est un outil important pour protéger l'intégrité et la fiabilité des documents judiciaires qui exigent une signature, lorsque les cours exercent leurs activités dans un environnement sans papier.

**Renvois :** ISO 27001:2013A.10. ISO 27017:2015, s. 10, ISO 27002, 10.1, *Règlement sur les signatures électroniques autorisées*, DORS/2005-30, pris en application de la *Loi sur la preuve au Canada* et de la *LPRPDE* : . (consulté le 21 janvier 2021)

## 18. MIGRATION VERS L'INFORMATIQUE EN NUAGE

**Politique 18a :** L'information judiciaire ne peut être migrée vers le nuage informatique sans le consentement de la magistrature et à moins que les conditions préalables obligatoires énoncées dans les *Lignes directrices sur l'informatique en nuage* ne soient respectées. Ainsi, la magistrature doit participer aux négociations concernant les services d'informatique en nuage proposés, y compris la gouvernance, les opérations, les contrôles d'accès, l'emplacement des données et d'autres considérations en matière de sécurité.

**Politique 18b :** Toute entente avec un fournisseur de services doit expressément traiter de la sécurité, de la confidentialité et de l'intégrité de l'*information judiciaire*. Le respect du Plan directeur par les tiers doit être surveillé et vérifié régulièrement.

**Commentaire :**

L'informatique en nuage permet aux utilisateurs de différentes organisations de partager le matériel, les services de réseau et les logiciels d'un même fournisseur, tout en permettant à chaque organisation de gérer elle-même son information et l'accès de ses utilisateurs de manière indépendante. Cela fait contraste avec les architectures traditionnelles, où chaque organisation construit son propre centre de données et se procure son propre équipement de réseau, son matériel informatique et ses logiciels. Grâce à la consolidation des investissements dans l'espace physique, la gestion, le matériel, les logiciels, les communications, l'alimentation électrique, la sauvegarde des données et la sécurité, les utilisateurs de l'informatique en nuage utilisent et

payent seulement les ressources informatiques dont ils ont besoin, laissant ainsi l'administration de la technologie au fournisseur de services.

Du point de vue du gouvernement, la consolidation permet de mieux contrôler la gestion des technologies et les dépenses en cette matière. Du point de vue de la magistrature, cependant, la consolidation des réseaux, de l'informatique et des services de soutien se traduit par une diminution du contrôle et une plus grande incertitude quant à la protection de l'*information judiciaire*. Pour cette raison, la magistrature de chacune des juridictions touchées a demandé plus de transparence et une plus grande participation aux processus de planification et de mise en œuvre.

En général, si l'organe exécutif va se charger de fournir des services d'information à la magistrature, que ce soit directement ou en association avec des tiers commerciaux, la magistrature doit jouer un rôle actif pour décider comment elle veut que l'*information judiciaire* soit gérée.

Dans les *Lignes directrices sur l'informatique en nuage*, le Conseil canadien de la magistrature a défini comme étant obligatoires les conditions préalables suivantes pour le transfert de l'*information judiciaire* au *nuage informatique* :

1. L'évaluation des menaces et des risques
2. L'évaluation des facteurs relatifs à la vie privée
3. La définition de l'*information judiciaire*
4. La définition de l'*utilisateur judiciaire*
5. La classification de l'*information judiciaire*
6. La résidence de l'information au Canada - [traduction] « Le lieu de résidence de l'information (y compris OneDrive et SharePoint) doit demeurer au Canada (lorsque l'information est immobile, y compris les copies de sauvegarde). Lorsque l'information est en transit, les données devraient résider au Canada, dans la mesure du possible. »
7. La gestion des documents
8. La formation

D'autres exigences sont énoncées dans ce document et devraient être consultées avant et après la migration de l'*information judiciaire*.

**Renvois :** NIST SP800-53r5, 18-SA, ISO 27001:2013, A.15, Cloud Security Alliance Security Guidance Version 4, (consulté le 21 janvier 2021). Voir aussi *Centre de la sécurité des télécommunications*, ITSB-105 Recours à des services contractuels d'infonuagique publique : implications sur le plan de la sécurité - décembre 2014), (consulté le 21 janvier 2021)

**CCM :** *Lignes directrices sur la migration de l'information judiciaire vers un fournisseur de services d'informatique en nuage* (2019). (consulté le 12 février 2021)

## 19. EMPLACEMENT DES DONNÉES

**Politique 19 :** L'*information judiciaire classifiée* doit être stockée dans une installation informatique située dans les limites géographiques du Canada. L'*information judiciaire classifiée* ne peut être exposée au risque qu'une quelconque autorité policière étrangère y obtienne accès, sans qu'il y ait une évaluation des menaces et des risques et une évaluation des facteurs relatifs à la vie privée, et sans l'autorisation préalable de la magistrature.[10]

**Commentaire :**

L'*information judiciaire classifiée* (telle que décrite dans la Politique 16 et ses commentaires doit résider en tout temps au Canada. Les *utilisateurs judiciaires* doivent être avisés et donner leur consentement préalable s'il est proposé que des *données judiciaires* quelconques soient stockées, traitées ou transmises hors des juridictions canadiennes ou par des hôtes au Canada qui sont assujettis à des lois étrangères attentatoires. Les *informations judiciaires* destinées à être accessibles au public (c'est-à-dire les informations non classifiées ou déclassifiées) ne sont soumises à aucune restriction de localisation liée à la sécurité.

[10] À titre de bon exemple, la *Clarifying Lawful Overseas Use of Data Act*, ou *CLOUD Act*, (H.R. 4943) est une loi fédérale des États-Unis promulguée en 2018 par l'adoption de la *Consolidated Appropriations Act*, 2018, PL 115-141, article 105 *Executive Agreements on Access to Data by Foreign Governments*. Essentiellement, la *CLOUD Act* modifie la *Stored Communications Act* (SCA) de 1986 afin de permettre aux organismes fédéraux d'application de la loi d'obliger les entreprises de technologie basées aux États-Unis, au moyen d'un mandat ou d'une assignation, à fournir les données demandées stockées sur des serveurs, que les données soient stockées aux États-Unis ou à l'étranger. Voir Wikipédia : https://fr.wikipedia.org/wiki/CLOUD_Act. (consulté le 21 janvier 2021)

**Renvois :** Conseil du Trésor, Souveraineté des données et nuage public (consulté le 21 janvier 2021).

*Évaluation et autorisation de sécurité*. NIST SP800-53r5, 15-CA (emplacement des données).

## 20. PROCÉDURES VIRTUELLES – VIDÉOCONFÉRENCE ET DIFFUSION EN CONTINU

**Politique 20a :** Les plateformes de vidéoconférence utilisées pour les procédures judiciaires doivent être suffisamment sécurisées pour être conformes au Plan directeur. Toute plateforme de vidéoconférence servant aux procédures judiciaires doit être soigneusement configurée et testée à l'avance pour veiller à ce que les procédures ne soient pas perturbées. Les utilisateurs finals (y compris les membres du public) devraient être informés du protocole des audiences vidéo établi par le juge président.

**Politique 20b :** La largeur des bandes passantes pour l'accès à Internet dont disposent les *utilisateurs judiciaires* d'un palais de justice doit être suffisante pour assurer une très bonne performance vidéo et audio.

**Politique 20c :** Dans la mesure où des procédures multimédias par vidéoconférence doivent être enregistrées, y compris le contenu textuel connexe, une capacité de stockage de données suffisante et sécurisée doit être fournie, selon les exigences du Plan directeur et en conformité avec la classification de l'information.

**Politique 20d :** Les procédures par vidéoconférence qui ont été déclassifiées par le ou les juges présidents peuvent être affichées sur des plateformes publiques de partage de vidéos, comme YouTube ou Vimeo, à condition que les réglages, les marques numériques et les indications appropriés soient affichés pour refléter les politiques de la cour en matière d'accès public et d'utilisation.

**Commentaire :**

La pandémie de la Covid-19 a accéléré la transition des procédures judiciaires en personne aux procédures virtuelles, et du dépôt de documents imprimés au dépôt par voie électronique. Les cours ont rapidement adopté la vidéoconférence, que ce soit en élargissant leurs systèmes internes existants (comme Microsoft Teams ou Webex) pour permettre aux utilisateurs externes

d'y avoir accès, ou en obtenant une licence d'utilisation de plateformes commerciales spécialisées comme Zoom.

Les *utilisateurs judiciaires* qui exercent leurs activités au sein de la cour ou à distance devraient disposer autant que possible d'une largeur de bandes passantes constantes et suffisantes pour que les connexions vidéo et audio puissent fonctionner sans interruption ni interférence.

Les fournisseurs de plateformes de vidéoconférence ont publié diverses lignes directrices et pratiques exemplaires en matière de sécurité pour protéger leurs plateformes respectives contre les interventions importunes et d'autres perturbations. Il est conseillé de les suivre attentivement.

Certains tribunaux ont adopté des scripts pour les juges qui président, qui peuvent être lus à tous les participants au début d'une audience virtuelle afin d'orienter les utilisateurs vers un processus peu familier. Il est recommandé que ce script ou cette liste de contrôle comporte des références aux questions de sécurité telles que le respect de la vie privée, la confidentialité, les interdictions (si applicable) d'enregistrement et de diffusion en continu des procédures ainsi que les configurations de l'équipement local, le cas échéant.

**Renvois :** NSA, *Selecting and Safely Using Collaboration Services for Telework* – UPDATE (Nov. 2020), Recommandations de Zoom (consulté le 21 janvier 2010), Sécurité dans Microsoft Teams : (consulté le 21 janvier 2010), Cisco Webex Meetings Security : (consulté le 21 janvier 2021).

## 21. PROCÉDURES VIRTUELLES – COLLABORATION (PARTAGE DE FICHIERS)

**Politique 21a :** Lorsqu'il s'agit d'obtenir, de configurer et de mettre en place des outils de collaboration, comme les logiciels de partage de fichiers et de documents pour les procédures virtuelles, les cours doivent s'assurer de disposer d'une capacité de stockage suffisante et de mettre en place des mesures de sécurité adéquates pour le téléchargement, le partage et le stockage de données. Ces mesures peuvent comprendre le chiffrement de l'information classifiée, ainsi qu'une piste de vérification des opérations de téléchargement, de récupération, de modification et de suppression de fichiers.

**Politique 21b :** Les cours doivent veiller à ce que les utilisateurs finals soient dûment authentifiés afin d'éviter tout accès non autorisé.

**Commentaire :**

En dépit de la commodité attrayante et du faible coût (ou de la gratuité) des plateformes publiques de partage de fichiers, comme Dropbox, Box.com et beaucoup d'autres, les cours qui ont l'intention de partager de l'information classifiée pour les besoins des procédures virtuelles devraient éviter les plateformes grand public, à moins que leur sécurité n'ait été pleinement vérifiée. Il convient d'envisager le concept d'un "nuage communautaire pour les juges" canadien - dans lequel le pouvoir judiciaire aurait sa propre location indépendante, spécifiquement à des fins telles que la collaboration virtuelle.

**Renvois : CCM :** *Lignes directrices sur la migration de l'information judiciaire vers un fournisseur de services d'informatique en nuage* (2019). (consulté le 12 février 2021)

## 22. MÉDIAS SOCIAUX

**Politique 22 :** La magistrature est responsable de l'établissement des politiques de sécurité, des codes de conduite et des programmes de formation pour l'utilisation des médias sociaux par les *utilisateurs judiciaires*.

**Commentaire :**

Les réseaux et les médias sociaux posent de nombreux défis aux cours et à la magistrature, particulièrement en ce qui concerne la sécurité et la protection de la vie privée. Parmi ceux-ci, mentionnons [traduction] « les contrôles d'authentification insuffisants, les scripts intersites, la falsification de requêtes intersites, l'hameçonnage, les fuites d'information, l'injection de code, l'intégrité de l'information et l'anti-automatisation insuffisante. »[11] Les politiques et les activités de formation devraient porter sur tous les risques connus.

[11] Cité par Wu He, (2012), "A review of social media security risks and mitigation techniques", Journal of Systems and Information Technology, Vol. 14, Issue 2, pp. 171-180. https://www.researchgate.net/publication/263528558_A_review_of_social_media_security_risks_and_mitigation_techniques (consulté le 21 janvier 2021).

## 23. CONFORMITÉ

**Politique 23a :** Toutes les politiques, procédures et pratiques en matière d'*information judiciaire* doivent être conformes aux lois et règlements applicables et aux exigences contractuelles valides. L'accès aux outils de vérification de conformité et leur utilisation doivent être limités seulement à un petit nombre de personnes autorisées. Lorsque l'*information judiciaire* et les *utilisateurs judiciaires* font l'objet d'une vérification de conformité, celle-ci doit se faire conformément aux *Lignes de conduite sur la surveillance informatique*.

**Politique 23b :** Dans les circonstances où il pourrait être nécessaire de fouiller l'*information judiciaire* ou d'y avoir accès en réponse à une demande juridique, l'autorisation préalable de la magistrature doit être obtenue. La magistrature doit déterminer qui peut obtenir accès à l'information judiciaire et quels éléments d'*information judiciaire* peuvent être exemptés des processus de fouille, d'examen et de divulgation.

**Commentaire :**

Il est important que toute personne chargée de l'audit de conformité - qu'elle travaille pour le compte des tribunaux, d'un service de l'administration des tribunaux, d'un ministère ou d'un tiers commercial - soit autorisée par le pouvoir judiciaire et informée au préalable de la méthode et de l'étendue des travaux. Les personnes qui effectuent ce travail doivent être informées de l'obligation de se conformer aux lignes directrices en matière de contrôle. Ces conditions doivent faire partie de tout protocole d'entente ou de tout accord d'hébergement de données par un tiers.

Que l'*information judiciaire* soit exemptée ou non d'une demande de divulgation dans le cadre d'un litige ou d'une demande d'accès à l'information, dans quelque circonstance que ce soit, le processus de fouille, d'examen et de production de l'*information judiciaire* ne doit être accompli que par la magistrature, ou avec son consentement et sous sa surveillance directe.

**Renvois :** NIST SP800-53r5, 2-AU, 16-AU, ISO 27001:2013, A.18.

**Cadre de politique :** Une évaluation des facteurs relatifs à la vie privée doit avoir lieu au stade de conception des systèmes de gestion de l'information judiciaire qui pourraient servir à recueillir, à

récupérer, à utiliser ou à diffuser des renseignements personnels. (Politique de protection de la vie privée n° 3)

L'accès aux outils de vérification de conformité et leur utilisation doivent être limités seulement à un petit nombre de personnes autorisées. Les listes de contrôle doivent être surveillées de près afin de pouvoir identifier facilement les utilisateurs qui ont accès à l'information judiciaire à n'importe quel moment. (Politique de sécurité n° 3)

# ANNEXE 1 : PRINCIPAUX RENVOIS

Le *Cadre de politique* offre une structure fondée sur des principes pour établir un large éventail de politiques concernant l'*information judiciaire*, dont la sécurité de l'information n'est qu'un aspect. La mise à jour du Plan directeur consiste donc, en partie, à assurer sa conformité avec les valeurs, principes, politiques et définitions énoncés dans le *Cadre de politique*, auquel le lecteur du Plan directeur devrait se référer.

Sauf indication contraire, les renvois indiqués dans chaque section des politiques du Plan directeur font référence aux documents suivants :

## PUBLICATIONS DU CONSEIL CANADIEN DE LA MAGISTRATURE

- *Court Information Management Policy Framework to Accommodate the Digital Environment*, Jo Sherman, 2013. (consulté le 21 janvier 2021) ("Framework")
- *Cadre de politique de gestion de l'information judiciaire dans le monde numérique*, Jo Sherman, 2013. (consulté le 21 janvier 2021) (« Cadre de politique »)
- *Guidelines for Migration of Judicial Information to a Cloud Service Provider*, Martin Felsky, 2019. (consulté le 21 janvier 2021) ("Cloud Guidelines")
- *Lignes directrices sur la migration de l'information judiciaire vers un fournisseur de services d'informatique en nuage*, Martin Felsky, 2019, (consulté le 21 janvier 2021) (« Lignes directrices sur l'informatique en nuage »)
- *Model Definition of Judicial Information*, Martin Felsky, 2020, (consulté le 21 janvier 2021) ("Model Definition")
- *Définition modèle des renseignements de la magistrature*, Martin Felsky, 2020, (consulté le 21 janvier 2021) (« Définition modèle »)
- Computer Monitoring Guidelines, 2002, (consulté le 21 janvier 2021) ("Monitoring Guidelines")
- Lignes de conduite sur la surveillance informatique, 2002, (« Lignes de conduite sur la surveillance informatique »)

## NORMES ET PRATIQUES EXEMPLAIRES INTERNATIONALES

- *Systèmes de management de la sécurité de l'information*, ISO/IEC 27001:2013. Le dernier examen de cette norme date de 2019. (consulté le 21 janvier 2021). La version de 2017 est très semblable et peut servir de référence à la place de celle de 2013.
- *Technologies de l'information - Techniques de sécurité - Code de bonne practique pour le management de la sécurité de l'information*, ISO/IEC 27002:2013. (consulté le 21 janvier 2021)
- *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publications SP800-53r5 – version de septembre 2020, y compris les mises à jour en date du 2020-12-10 - (consulté le 21 janvier 2021)
- *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* NIST Special Publications SP800-171 Rev. 2 (publié en février 2020), (consulté le 21 janvier 2021)
- *UK Cabinet Office, Government Security Classifications*, mai 2018 version 1.1, (consulté le 21 janvier 2021)

## NORMES DE CERTAINES JURIDICTIONS CANADIENNES

- *British Columbia Information Security Policy* V4.0, dernière révision 2018-09-21: (consulté le 21 janvier 2021)
- Exigences générales en matière de sécurité en vue de protéger l'intégrité, la confidentialité et la disponibilité des réseaux et des systèmes informatiques du gouvernement de l'Ontario (consulté le 21 janvier 2021)
- Canadian Centre for Cyber Security (consulté le 21 janvier 2021); Centre canadien pour la cybersécurité (consulté le 21 janvier 2021)

## ANNEXE 2 : RECOMMANDATIONS DU COMITÉ CONSULTATIF SUR LA TECHNOLOGIE (CCT) APPROUVÉES PAR LE CONSEIL, 30 NOV. 2001

1. Que le Conseil canadien de la magistrature tienne un séminaire à sa prochaine réunion semestrielle sur les questions urgentes de sécurité mises au jour dans le présent rapport (Sécurité technologique dans les cours : rapport du Comité consultatif sur la technologie).

2. Que le président du Conseil canadien de la magistrature transmette le présent rapport au Conseil canadien des juges en chef.

3. Que le président du Conseil canadien de la magistrature transmette le présent rapport aux sous-procureurs généraux et leur demande de collaborer à la mise en œuvre des recommandations.

4. Que le Conseil canadien de la magistrature demande à l'Institut national de la magistrature et au Commissariat à la magistrature fédérale de coordonner la formation (sur les questions de sécurité du système d'information, y compris les préoccupations relatives à l'indépendance judiciaire et à l'intégrité de l'*information judiciaire*) à l'intention des juges fédéraux et provinciaux ainsi que du personnel des technologies de l'information.

5. Que le Conseil canadien de la magistrature demande à tous les juges en chef de nomination fédérale ou provinciale :

    a) de donner la priorité à la sécurité du système d'information des cours;

    b) de veiller à l'élaboration immédiate d'une politique de sécurité, avant la conversion à un système électronique;

    c) d'identifier et d'obtenir les ressources financières, le personnel et les autres ressources nécessaires qui sont essentielles à la mise en œuvre des mesures de sécurité appropriées;

    d) de faire en sorte qu'un membre du personnel des technologies de l'information relevant du juge en chef soit nommé pour gérer la sécurité informatique des cours.

6. Pour des besoins d'uniformité, que le Conseil canadien de la magistrature assume un rôle de direction en autorisant le Comité consultatif sur la technologie à élaborer un plan directeur portant sur les mesures de sécurité recommandées pour toutes les cours canadiennes, et qu'il fasse en sorte que le comité dispose des ressources nécessaires à cette fin.

---

## ANNEXE 3 : GLOSSAIRE DE TERMES TECHNIQUES ET D'ACRONYMES

| Terme | Signification |
|---|---|
| MPA – Menaces persistantes avancées | Intrusions de haut niveau dans des réseaux informatiques qui persistent pendant de longues périodes sans être détectées.[12] |
| Analytique | L'application d'outils logiciels avancés servant à découvrir et à extraire de l'information significative parmi de grandes quantités de données. |
| Anonymisation | Processus qui consiste à supprimer les renseignements personnels contenus dans des ensembles de données. |
| Appli | Application logicielle conçue pour être téléchargée et fonctionner sur un appareil mobile. |
| PAP | Signifie « Prenez vos appareils personnels », une politique qui permet aux utilisateurs d'accéder à des réseaux d'entreprise au moyen d'appareils mobiles personnels qui leur appartiennent. |
| Nuage | Terme employé pour désigner des centres de données gérés par des tiers (fournisseurs de services d'informatique en nuage) qui hébergent les données d'une organisation dans un lieu externe. |
| FSIN | Fournisseur de services d'informatique en nuage. Microsoft Azure et Amazon Web Services sont les deux plus importants FSIN ayant des centres de données situés au Canada. |
| Signature numérique | Une signature numérique est un message encodé qui identifie spécifiquement son expéditeur et qui prouve que le message n'a pas changé depuis qu'il a été transmis. Voir signature électronique. |
| Chiffrement | Processus qui consiste à transformer un texte en clair en un code inintelligible dans le but de protéger l'information contre l'accès non autorisé. |
| Signature électronique (voir signature numérique) | Une signature électronique est une forme de signature appliquée à un document électronique, qui se distingue parfois d'une signature numérique, laquelle est une forme d'authentification encodée. |
| Pare-feu | Dispositif matériel ou logiciel conçu pour protéger un ordinateur ou un |

[12] Selon une étude de Bell Canada ("The Dark Space Project", 2013), la présence très répandue de menaces persistantes avancées (MPA) a été découverte dans les infrastructures du gouvernement canadien et les infrastructures essentielles : http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf (consulté le 21 janvier 2021).

| Terme | Signification |
|---|---|
| | réseau contre les tentatives d'intrusion extérieures. |
| SDI | Système de détection d'intrusion – un système qui surveille les tentatives d'accès non autorisé à un réseau. L'intrusion est définie comme une tentative de compromettre la sécurité d'un ordinateur ou d'un réseau. La détection d'intrusion est le processus qui consiste à surveiller les activités effectuées dans un système ou un réseau informatique et à les analyser pour détecter les tentatives d'intrusion. |
| Intégrité | L'intégrité est le besoin de s'assurer que l'information n'a pas été changée accidentellement ou délibérément et qu'elle est exacte et complète. |
| FSI | Fournisseur de services Internet – une organisation qui fournit des services d'accès à Internet. |
| Réseau local | Système qui relie des utilisateurs à des ressources informatiques partagées à l'intérieur d'un bâtiment. |
| Droit d'accès minimal | Principe consistant à accorder aux utilisateurs ou aux applications seulement les permissions nécessaires à l'exercice de leurs fonctions autorisées. |
| Code malveillant | Programmes ou codes conçus pour effacer des données, empêcher l'accès ou autrement nuire au bon fonctionnement d'un système informatique – terme générique désignant les virus et vers informatiques, les logiciels espions, les chevaux de Troie, les logiciels malveillants, les attaques par déni de service, etc. |
| Logiciel malveillant | Terme générique désignant un certain nombre de différents types de codes malveillants. Voir code malveillant. |
| Hameçonnage | Utilisation de courriels falsifiés pour amener les destinataires à visiter des sites Web contrefaits et conçus pour les tromper et les convaincre de divulguer des données personnelles. En général, le courriel et le site Web falsifiés se font passer pour une institution financière avec laquelle l'utilisateur fait affaire. |
| Sécurité physique | La sécurité physique désigne la protection des sites et de l'équipement (et de l'information et des logiciels qu'ils contiennent) contre l'introduction par effraction, le vol, le vandalisme, les catastrophes naturelles ou autres, et les dommages accidentels. |
| Infrastructure à clé publique (ICP) | Une infrastructure à clé publique (ICP) permet aux utilisateurs d'un réseau public non sécurisé, comme Internet, d'échanger des données et de l'argent de manière sûre et privée à l'aide d'une paire de clés de chiffrement (une clé publique et une clé privée) délivrées par une autorité de certification de confiance. L'infrastructure à clé publique repose sur l'utilisation de certificats numériques qui permettent d'identifier une personne ou une organisation ainsi que les services de répertoire pouvant stocker et, si nécessaire, annuler les certificats. |
| Logiciel rançonneur | Type de logiciel malveillant qui est une forme d'extorsion. Il permet de chiffrer le disque dur de l'ordinateur d'une victime pour l'empêcher d'avoir accès aux principaux fichiers. La victime doit ensuite payer une rançon pour pouvoir déchiffrer les fichiers et les récupérer. |

| Terme | Signification |
|---|---|
| Contrôle d'accès basé sur les rôles | Le contrôle d'accès basé sur les rôles attribue aux utilisateurs des rôles basés sur leurs fonctions organisationnelles et détermine les autorisations d'accès en fonction de ces rôles. |
| Services partagés | Modèle selon lequel des services d'informatique et de réseau sont fournis à l'ensemble d'une entreprise (comme un gouvernement) par la voie d'une seule ressource centralisée, au lieu de donner à chaque composante de l'entreprise sa propre infrastructure de TI. |
| Entente de niveau de service | L'entente de niveau de service sert à établir une compréhension commune des services, des priorités, des responsabilités et des garanties; elle prévoit généralement un « niveau de service » minimum à l'égard de la disponibilité, de la serviabilité, de la performance, du fonctionnement ou des autres aspects du service. |
| Piratage psychologique | Moyens non techniques ou peu technologiques - comme le mensonge, l'usurpation d'identité, la tromperie, la corruption, le chantage et les menaces - utilisés pour attaquer des systèmes d'information. |
| Escroquerie en ligne | Tentative d'une entité non autorisée pour obtenir accès à un système en se faisant passer pour un utilisateur autorisé. |
| Évaluation des menaces et des risques (EMR) | Processus qui consiste à définir les risques et à en déterminer l'impact. Une menace est une atteinte potentielle à la sécurité qui résulte de la présence d'une circonstance, d'une capacité, d'une action ou d'un événement pouvant violer la sécurité et causer du tort. |
| Cheval de Troie | Programme malveillant dissimulé à l'intérieur d'un autre programme en apparence inoffensif, qui exécute des opérations nuisibles à l'insu de l'utilisateur. |
| Virtualisation | La configuration d'une seule unité centrale de traitement (UCT) pour faire fonctionner plus d'un système d'exploitation à la fois, permettant ainsi à une entreprise de mieux gérer les mises à niveau et les changements rapides du système d'exploitation et des applications. |
| Virus | Programme malveillant qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un événement donné. |
| Réseau privé virtuel (RPV) | Réseau de communication privé et sécurisé qui se sert de l'infrastructure d'un réseau public pour transmettre des données protégées, généralement par chiffrement ou encapsulation. Par exemple, une entreprise possédant plusieurs établissements peut préférer utiliser les réseaux téléphoniques publics ou Internet en bénéficiant de son propre plan de numérotation ou d'adressage, plutôt que de se doter d'autocommutateurs privés et de moyens propres de transmission. |
| Confidentialité équivalente aux transmissions par fil (WEP) | Protocole de sécurité des réseaux locaux sans fil défini dans la norme IEEE 802.11b. |

| Terme | Signification |
|---|---|
| Réseau local sans fil | Réseau local permettant de relier des appareils informatiques sans fil, c'est-à-dire par des liaisons radioélectriques. |
| Ver informatique | Programme malveillant indépendant, capable de se reproduire par lui-même, qui se transmet d'un ordinateur à un autre par Internet ou tout autre réseau et qui perturbe le fonctionnement des systèmes en s'exécutant à l'insu des utilisateurs. |