Plan d'action en matière de sécurité des renseignements judiciaires

Cinquième édition, 2018

Préparé par Martin Felsky, Ph. D., J.D., pour le Comité exécutif du Conseil canadien de la magistrature, le 31 août 2018

TABLE DES MATIÈRES

INTRODUCTION À LA CINQUIÈME ÉDITION

Pour répondre aux préoccupations relatives à la sécurité au début des années 2000, le premier Plan d'action avait trois objectifs :

1. Fournir des lignes de conduite afin d'améliorer la sécurité, l'accessibilité et l'intégrité des renseignements judiciaires.
2. Définir les rôles et responsabilités respectifs des juges et des administrateurs en ce qui concerne la sécurité des technologies de l'information et à améliorer les relations entre les deux groupes.
3. Fournir aux juges de l'ensemble du Canada un modèle pour l'élaboration de politiques efficaces relatives à la sécurité des technologies de l'information qui tiennent compte des principes de l'indépendance judiciaire.

Aujourd'hui, il est juste de dire que, bien que ces trois objectifs soient toujours aussi valables, leur priorité relative a changé.

Les gouvernements et les organisations du secteur privé ont facilement accès à des normes complètes de programme de sécurité et à des contrôles de sécurité normatifs, et ils les utilisent largement. L'intérêt pour la cybersécurité, qui met l'accent sur les menaces provenant d'Internet, a connu une croissance explosive. Le défi d'aujourd'hui consiste à comprendre, à interpréter et à appliquer les principes de l'indépendance judiciaire de façon rentable, surtout à mesure que les gouvernements s'orientent vers la centralisation des plateformes technologiques pour l'ensemble de la fonction publique.

Les rôles distincts des juges et des administrateurs sont encore imprécis, bien que le paysage ait changé en vingt ans. À l'heure actuelle, presque toutes les administrations comptent un agent de la sécurité informatique du système judiciaire (« ASISJ »), conformément à la recommandation du Conseil.[1]

Les lacunes dans les politiques qui existent depuis un certain temps sont de plus en plus graves à mesure que les gouvernements centralisent les plateformes technologiques et planifient leur migration vers le nuage. Au-delà de la portée étroite de la sécurité, les questions de gouvernance plus large des renseignements judiciaires doivent être mises en lumière plus rapidement.

ATTESTATION

Le Plan d'action a été rédigé en consultation avec un groupe national d'agents de la sécurité des technologies de l'information judiciaire, que le Conseil remercie sincèrement.

[1] Au moment de la rédaction du présent document, des ASISJ ont été nommés dans huit des dix provinces, deux des trois territoires, les cours fédérales et la Cour suprême du Canada.

INTRODUCTION À LA QUATRIÈME ÉDITION, 2013

Le présent Plan d'action vise plusieurs objectifs, dont le principal consiste à fournir des lignes de conduite afin d'améliorer la sécurité, l'accessibilité et l'intégrité des renseignements judiciaires. Il vise également à définir clairement les rôles et responsabilités respectifs des juges et des administrateurs en ce qui concerne la sécurité des technologies de l'information et à améliorer les relations entre les deux groupes. Enfin, le Plan d'action est conçu de manière à fournir aux juges de l'ensemble du Canada un modèle pour l'élaboration de politiques efficaces relatives à la sécurité des technologies de l'information qui tiennent compte des principes de l'indépendance judiciaire.

Le Conseil canadien de la magistrature (le Conseil) est heureux que, depuis la publication de la première édition du Plan d'action en 2004, de nombreuses cours aient adopté des politiques de sécurité inspirées du Plan d'action et compatibles avec celui-ci.[2] À l'origine, le Conseil était préoccupé par le fait que le niveau de sécurité des renseignements judiciaires dans l'ensemble du Canada était inégal et différent d'une juridiction à l'autre, mais ces préoccupations ont maintenant été résolues en grande partie. Le Conseil est d'avis que les cours et les juges devraient continuer d'uniformiser l'approche à l'égard de la sécurité des renseignements judiciaires le plus possible parmi l'ensemble des cours. Des pratiques exemplaires doivent être arrêtées, mises en œuvre et tenues à jour dans tous les cas.

Le Conseil est également préoccupé par le fait que, dans certaines cours, les juges ne participent peut-être pas à la formulation des politiques. Le Conseil veut s'assurer que les juges jouent un plus grand rôle dans l'élaboration des politiques et que toutes les mesures de sécurité prises par les cours soient compatibles avec les principes fondamentaux de l'indépendance judiciaire.

Pour les juges, la sécurité des renseignements présente des défis d'ordre pratique en raison de la situation constitutionnelle unique du Canada. Par exemple, dans la plupart des cours, des administrateurs qui ne relèvent pas de l'autorité judiciaire fournissent tous les services informatiques aux juges. Non seulement la ligne qui sépare les juges et ces administrateurs est-elle mal définie, mais il est rare qu'un lien hiérarchique existe entre les deux groupes. C'est ce qui explique qu'il est parfois difficile pour les administrateurs d'obtenir la collaboration des juges sur le plan de l'application d'une politique informatique, tout comme il peut être difficile pour les juges de diriger les travaux du personnel de soutien technique.

Le Conseil suggère que les administrateurs de l'informatique, le personnel de soutien et le personnel des services de dépannage qui travaillent avec les utilisateurs judiciaires soient mis au

[2] Au moment de mettre sous presse, les cours de la Colombie-Britannique, de l'Alberta, de la Saskatchewan, de l'Ontario, du Québec, du Nouveau-Brunswick, de la Nouvelle-Écosse et de l'Île-du-Prince-Édouard ont mandaté des personnes ou des équipes pour jouer le rôle décrit dans le plan d'action sous le vocable « agent de la sécurité informatique du système judiciaire ». La Cour suprême du Canada et le Service administratif des tribunaux judiciaires du gouvernement fédéral ont également mandaté des personnes pour tenir ce rôle.

courant de la nature du rôle et de la fonction judiciaires dans le cadre de l'administration de la justice. Toutes ces personnes doivent faire la distinction entre les utilisateurs judiciaires et les autres utilisateurs afin de préserver l'indépendance judiciaire.

Le Conseil canadien de la magistrature a donné suite à plusieurs recommandations qui ont été formulées en novembre 2001[3] 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.
- 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 des utilisateurs finaux.
- 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 judiciaires est une fonction judiciaire et relève donc de la magistrature.
- La gestion, l'exploitation et les mesures techniques visant à protéger les renseignements judiciaires conformément à la politique judiciaire sont des fonctions administratives qui relèvent, dans le cas de la plupart des cours, du gouvernement provincial.[4]

Plus récemment, le Conseil a adopté seize politiques fondamentales touchant la gouvernance de l'information judiciaire, qui sont énoncées dans le Cadre de politique de gestion de l'information judiciaire dans le monde numérique (« le Cadre »). On y énonce également des politiques relatives à l'accès, à la protection de la vie privée, à la sécurité, à la préservation et à la mesure du rendement. Le Plan d'action a été réécrit pour qu'il soit conforme aux politiques du Cadre.

Le Plan d'action constitue une partie de l'approche du Conseil à l'égard de la sécurité des renseignements judiciaires. Le site Web du Conseil (www.cjc-ccm.gc.ca) présente de plus amples renseignements sur les initiatives connexes.

PORTÉE ET DÉFINITIONS

[3] Voir l'annexe 1. Le rapport complet de 2001 est confidentiel, car il traite des vulnérabilités des systèmes judiciaires.

[4] Bien que cette question ne se pose pas dans le cas des cours fédérales, comme la Cour suprême du Canada, le gouvernement fédéral considère que la fourniture de services d'accès Internet (par l'entremise de SCNet) constitue une fonction gouvernementale.

DÉFINITIONS

UTILISATEUR JUDICIAIRE

Selon la définition donnée dans le Cadre[5], l'officier de justice est « une personne qui agit à titre judiciaire ou quasi judiciaire, y compris les juges, les juges suppléants, les conseillers-maîtres, les juges de paix, les greffiers, les protonotaires ou toute autre personne autorisée à remplir une fonction judiciaire ou quasi judiciaire ». Dans ce plan d'action, l'expression « utilisateur judiciaire » englobe les officiers de justice et l'ensemble des personnes ayant accès à l'information judiciaire.

INFORMATION JUDICIAIRE

Il n'existe pas de définition largement acceptée de « l'information judiciaire ». Le Cadre aborde cependant la question de la définition de l'information judiciaire. On y note que la notion d'information judiciaire peut chevaucher des expressions définies comme « dossier d'instance » ou « dossier de la cour », qui sont des catégories de l'information judiciaire. Le Conseil propose d'utiliser les définitions du Cadre comme modèles permettant d'assurer une certaine uniformité entre les administrations. Les définitions suivantes sont maintenant utilisées dans le Plan d'action :

L'**information judiciaire** est l'information qui est stockée, reçue, produite ou utilisée par un officier de justice ou à son intention. Cela comprend aussi l'information qui est stockée, reçue, produite ou utilisée par ou pour le personnel de la cour ou les entrepreneurs qui travaillent directement pour les juges ou en leur nom, par exemple les cadres dirigeants, les techniciens juridiques, les étudiants en droit, les commis judiciaires ou les adjoints judiciaires.[6]

Il y a trois principaux types d'information judiciaire :

L'***information judiciaire individuelle*** comprend les produits des travaux, les documents de recherche et l'information concernant le perfectionnement professionnel des avocats-conseils internes, des techniciens juridiques et des officiers de justice. Cette catégorie engloberait aussi l'**information concernant la fonction judiciaire**, qui comprend les affaires de ressources humaines du personnel de la cour, l'information sur l'attribution des causes, les statistiques et les politiques de la cour. Les activités relatives à la participation à un comité judiciaire relèveraient aussi de cette définition.

[5] Jo Sherman, Cadre de politique de gestion de l'information judiciaire dans le monde numérique, Conseil canadien de la magistrature, 2013, http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Information%20Judiciaire%20dans%20le%20monde%20num%C3%A9rique%202013-03.pdf.

[6] Pour les besoins du Plan d'action, nous proposons d'ajouter également les « avocats-conseils à l'interne » à ce groupe.

L'***information judiciaire générale*** comprend l'information utilisée par les juges en chef, les documents des comités, les statistiques, les documents de recherche et l'information concernant le perfectionnement professionnel pour l'ensemble de la cour.

L'***information judiciaire personnelle*** comprend l'information produite par un officier de justice ou en son nom, ou l'information le concernant, qui n'est pas directement liée aux fonctions ou au rôle de l'officier de justice et qui n'est pas associée à une affaire.[7]

Dans ce contexte, les éléments d'information suivants seraient considérés comme de l'information judiciaire[8] :

- l'information concernant les affaires personnelles ou privées et les relations sociales des juges;
- les travaux concernant un dossier d'instance qui sont de nature très confidentielle (p. ex. les projets de jugement);
- les registres de contrôle qui contiennent des sommaires des activités informatiques des juges;
- l'historique des sites Internet consultés par les juges;
- la correspondance par courriel des juges qui n'est pas directement liée à un dossier d'instance;
- tous les messages textes et la messagerie vocale;
- tous les événements inscrits dans un agenda ou un calendrier, sauf les événements inscrits au registre de la cour, qui sont directement liés à un dossier d'instance;
- les coordonnées de personnes, y compris l'information contenue dans des carnets d'adresses électroniques et enregistrée dans des téléphones mobiles, des applications logicielles de bureau ou d'autres dépôts électroniques;
- l'information échangée par la voie de réseaux sociaux qui n'est pas du domaine public, par exemple les blogues privés et les réseaux collectifs fermés qu'utilisent les juges et leurs collègues professionnels;
- l'information concernant l'horaire des juges au rôle des audiences de la cour;
- le contenu des programmes de formation des juges;
- l'information concernant la participation d'un juge à des programmes de formation;
- les statistiques montrant les activités individuelles ou la charge de travail d'un juge;
- les notes personnelles, la recherche ou les documents de travail produits par un juge ou en son nom qui n'ont pas été versés à un dossier d'instance;

[7] Extrait du Cadre : « Chaque juridiction devra fournir des directives précises aux technologues à propos des fichiers de l'historique de navigation Internet, des dépôts de courriel, des listes de contacts, des calendriers, des messages textes et du courriel, lorsqu'il s'agira de choisir les éléments d'information à inclure dans cette catégorie [information juridique personnelle]. »

[8] Exemples tirés du Cadre, page 36-37.

- les activités relatives à la participation à des comités ou à des conseils judiciaires, y compris les communications et les documents de recherche;
- les cahiers d'audience des juges.

On doit se rappeler que l'information judiciaire doit être protégée non seulement sur les serveurs, appareils et dispositifs de stockage actifs, mais aussi sur les systèmes d'archives, d'images et de sauvegarde.

MAGISTRATURE

Le terme « magistrature » est utilisé dans l'ensemble du Plan d'action. Pour toute politique particulière, « la magistrature » peut désigner l'effectif des juges d'une cour particulière; le bureau du juge en chef d'une cour, un représentant désigné du juge en chef ou un comité de juges responsables de la technologie dans une administration.

PORTÉE

Même si le mandat légal du Conseil vise seulement les juges nommés par le gouvernement fédéral, il arrive souvent que ces juges partagent des plateformes et des ressources technologiques avec leurs collègues nommés par les gouvernements provinciaux. C'est pour cette raison, entre autres, que la collaboration à l'égard de l'élaboration des politiques en matière de sécurité est encouragée. Le Plan d'action s'applique à tout système informatique utilisé pour l'information judiciaire. Ceci peut comprendre les services infonuagiques, les ordinateurs à la maison, 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 le Plan d'action ne peut en couvrir tous les aspects. De plus, le Conseil s'intéresse principalement au rôle de la magistrature dans l'élaboration des normes et politiques et non pas aux détails de la gestion d'un service informatique. À cet égard, le Plan d'action ne couvre pas chacun des aspects de l'administration de la sécurité. Il ne traite pas non plus de la sécurité des renseignements qui ne sont pas sous forme numérique, de la sécurité des communications par téléphone ou par télécopieur, ni de la sécurité matérielle des palais de justice et de leurs occupants.

Le Plan d'action vise à adapter et à améliorer les politiques et programmes gouvernementaux existants. Dans cette mesure, le Plan d'action est conçu pour être utilisé conjointement avec les normes, lignes directrices et pratiques exemplaires mondiales en matière de sécurité informatique, dont certaines sont énumérées dans la section des principales références ci-dessous.

RÉSUMÉ DES PRINCIPAUX CHANGEMENTS APPORTÉS À LA CINQUIÈME ÉDITION

1. Une réorganisation générale et une mise à jour pour tenir compte des nouvelles technologies et des nouvelles priorités.
2. Élargissement des sections de commentaires.
3. Les politiques renvoient aux contrôles des normes ISO 27001/2:2013 et NIST SP800-53r5, le cas échéant.
4. Réponse aux commentaires et aux questions des intervenants.
5. Une nouvelle version du modèle de politique d'utilisation acceptable (annexe 4).
6. Remplace le modèle des modalités d'ENS par une référence plus utile.

POLITIQUES

1. INDÉPENDANCE JUDICIAIRE

Politique 1a : Toutes les mesures que prennent les cours en matière 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.

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 de réseau, la configuration, les contrôles d'accès et le soutien opérationnel doivent être conformes au Plan d'action.

Politique 1c : Peu importe qui en a la garde, la magistrature est toujours propriétaire de l'information judiciaire.

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. L'indépendance judiciaire comprend la protection de toute influence indue mais, surtout, l'indépendance vis-à-vis du pouvoir 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.[9] Étant donné qu'une

[9]« 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. » L'hon. Ian Binnie, « Judicial Independence in Canada », http://www.venice.coe.int/WCCJ/Rio/Papers/CAN_Binnie_E.pdf, page 34.

magistrature indépendante suscite la confiance du public dans le système de justice, l'*apparence* d'indépendance doit également être soigneusement préservée.

Renvois : NIST SP-800-171r1.

Cadre : Tous les juges et tout le personnel des cours devraient utiliser un domaine Internet commun qui est séparé de celui du gouvernement et ils devraient employer ce domaine pour toutes leurs communications (Politique fondamentale 8).

2. POLITIQUE

Politique 2a : La responsabilité relative aux politiques de sécurité en ce qui concerne les renseignements judiciaires est une fonction judiciaire et relève donc de la magistrature. La gestion, l'exploitation et les mesures techniques visant à protéger les renseignements judiciaires conformément à la politique judiciaire sont des fonctions administratives qui relèvent, dans le cas de la plupart des cours, d'une entité gouvernementale.

Politique 2b : Chaque tribunal doit planifier et mener une évaluation annuelle des menaces et des risques (« EMR ») en collaboration avec la magistrature. Le degré de détail requis dans une EMR et sa portée peuvent varier d'une cour à une autre, selon les circonstances.

Renvois : NIST SP800-53r5, 12-PL, 14-RA, ISO 27001:2013, A.5. Consultez la norme ISO/CEI 27005 pour obtenir des lignes directrices relatives à la gestion des risques.

Cadre : Un ensemble de modèles de politiques régissant la sécurité de l'information et la protection des renseignements personnels devrait être officiellement adopté, approuvé et publié par le Conseil canadien de la magistrature, en fonction des priorités établies dans le Plan d'action (Politique d'accès 7).

3. GOUVERNANCE

Politique 3 : La gestion de la sécurité de l'information judiciaire doit s'insérer dans un programme de sécurité formel et documenté, autorisé et adéquatement financé par l'instance gouvernementale responsable de l'administration judiciaire. L'administration judiciaire doit décrire dans un plan écrit comment les exigences de sécurité de la magistrature seront satisfaites.

Commentaire :

La sécurité de l'information judiciaire ne peut être laissée à des processus ad hoc, informels et non documentés, et sa responsabilité ne peut être déléguée à des employés subalternes. Des budgets adéquats doivent y être consacrés afin d'assurer la sécurité et l'intégrité de l'information judiciaire, selon l'évaluation de la menace et du risque.

Renvois : ISO 27001:2013, A.6.

4. AGENT DE LA SÉCURITÉ INFORMATIQUE DU SYSTÈME JUDICIAIRE

Politique 4 : Chaque juridiction doit veiller à ce qu'un agent de la sécurité informatique du système judiciaire (agent) responsable envers la magistrature soit nommé et chargé de surveiller la gestion des mesures de sécurité relatives aux technologies de l'information des cours.

Le rôle principal de l'agent consiste à fournir des avis à la magistrature dans le cadre de ses négociations et de son étroite coopération avec l'administration judiciaire et les fournisseurs tiers sur les questions relatives à la sécurité de l'information. L'élément clé est que l'agent est responsable devant la magistrature, idéalement de manière exclusive, pour éviter tout conflit d'intérêts potentiel. Dans certaines juridictions, l'agent peut faire partie d'une organisation qui offre du soutien aux utilisateurs judiciaires, et les qualifications, les rôles et les responsabilités spécifiques d'une équipe d'agents doivent être déterminés en fonction des besoins de chaque cour.

5. FORMATION ET SENSIBILISATION

Politique 5 : Une formation de base sur la protection des renseignements personnels et la sensibilisation à la sécurité doit être offerte à tous les utilisateurs du système, y compris les utilisateurs judiciaires, tandis qu'une formation plus poussée sur les rôles doit être offerte aux utilisateurs ayant accès aux renseignements judiciaires.

Commentaire :

La sensibilisation ainsi que la formation et l'éducation à la sécurité sont toutes nécessaires pour assurer le succès de tout programme relatif à la sécurité des renseignements. Le programme de formation devrait comprendre de la documentation sur l'indépendance de la magistrature et la position constitutionnelle particulière des utilisateurs judiciaires.

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

6. MIGRATION VERS L'INFORMATIQUE EN NUAGE

Politique 6a : Les renseignements judiciaires ne doivent pas être migrés vers le nuage sans le consentement de la magistrature. Par conséquent, la magistrature doit participer aux négociations visant les services en nuage proposés, y compris la gouvernance, les opérations, les contrôles d'accès, l'emplacement des données et d'autres considérations de sécurité. La sécurité, la protection des renseignements personnels et l'intégrité des renseignements judiciaires doivent être expressément abordées dans toute entente avec un fournisseur de services. La conformité des tiers au Plan d'action doit être surveillée et vérifiée régulièrement.

Commentaire :

L'informatique en nuage permet à différents utilisateurs dans différentes organisations de partager le matériel, les services de réseau et même des logiciels dans un même centre de données, chaque organisation gérant de façon indépendante ses propres accès d'utilisateurs et son information. Cette façon de faire s'oppose à l'architecture informatique traditionnelle, dans laquelle chaque organisme construit ses propres centres de données et se procure son propre équipement de réseau, son matériel informatique et ses logiciels. L'avantage de l'informatique en nuage tient au fait que la consolidation de l'investissement dans l'espace physique, la gestion, le matériel, les logiciels, les communications, l'alimentation électrique, la sauvegarde des données et la sécurité, permet aux utilisateurs de n'utiliser et de ne payer que la puissance informatique dont ils ont besoin, laissant l'administration de la technologie à leur fournisseur de services.

Du point de vue du gouvernement, la consolidation permet un meilleur contrôle sur les dépenses et la gestion technologiques. Du point de vue de la magistrature, par contre, la consolidation des réseaux, de l'informatique et des services de soutien se traduit par une diminution du contrôle et donc une plus grande incertitude à propos de la protection de l'information judiciaire. Pour cette raison, les magistrats de chacune des juridictions touchées ont demandé une plus grande transparence et une voix plus forte dans les processus de planification et de mise en œuvre.

En règle générale, si le pouvoir exécutif doit fournir des services d'information à la magistrature, que ce soit directement ou dans le cadre d'un partenariat avec des tiers fournisseurs, la magistrature doit jouer un rôle actif en précisant comment elle souhaite que l'information judiciaire soit gérée.

Renvois : NIST SP800-53r5, 18-SA, ISO 27001:2013, A.15, Cloud Security Alliance Security Guidance Version 4, https://cloudsecurityalliance.org/group/security-guidance/#_overview. Voir aussi Communications Security Establishment, ITSB-105 Security Considerations for the Contracting of Public Cloud Computing Services.

7. EMPLACEMENT DES DONNÉES

Politique 7 : Les renseignements judiciaires doivent être stockés dans une installation informatique située dans les limites géographiques du Canada. On ne peut prendre le risque que les renseignements judiciaires soient consultés par des autorités policières étrangères sans qu'il y ait une évaluation de la menace et des risques et une évaluation des facteurs relatifs à la vie privée et sans l'approbation préalable de la magistrature.[10]

Commentaire :

Les renseignements judiciaires doivent en tout temps être conservés au Canada. Les utilisateurs judiciaires doivent être avisés et donner leur consentement au préalable s'il est proposé que des données judiciaires soient stockées, traitées ou transmises hors des juridictions canadiennes ou par des hôtes au Canada qui sont assujettis à des lois étrangères intrusives.

Renvois : Conseil du Trésor, Orientation relative à la résidence des données électroniques, Avis de mise en œuvre de la Politique sur la TI 2017-02, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/orientation-relative-residence-donnees-electroniques.html. Évaluation et autorisation de sécurité. NIST SP800-53r5, 15-CA (emplacement des données).

[10] À titre d'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 Ententes exécutives sur l'accès aux données par des gouvernements étrangers. 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. Wikipédia à l'adresse https://fr.wikipedia.org/wiki/CLOUD_Act.

8. CONFORMITÉ

Politique 8a : L'ensemble des politiques, des procédures et des pratiques d'information judiciaire doit être conforme aux lois et aux règlements applicables et aux exigences contractuelles valides. L'accès aux outils de conformité et leur utilisation doivent être limités à un petit nombre de personnes autorisées seulement. Lorsque les vérifications portent sur l'information judiciaire et les utilisateurs judiciaires, elles doivent être faites conformément aux Lignes de conduite sur la surveillance informatique.

Politique 8b : Dans les cas où des renseignements judiciaires peuvent devoir être fouillés ou autrement consultés en réponse à une demande juridique, l'approbation préalable de la magistrature est requise. La magistrature détermine quels sont les utilisateurs qui ont accès aux renseignements judiciaires et quels sont les renseignements judiciaires qui peuvent être exemptés des processus de recherche, d'examen et de divulgation.

Commentaire :

Que les renseignements judiciaires, dans quelque circonstance que ce soit, soient exemptés ou non des demandes de divulgation et d'accès à l'information en cas de litige, le processus de recherche, d'examen et, à la toute fin, de production de renseignements judiciaires ne doit être effectué 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 : Des évaluations de l'incidence sur la protection de la vie privée seront réalisées à l'étape de la conception de systèmes de gestion de l'information des cours qui tiennent compte de la collecte potentielle, de l'accès, de l'utilisation ou de la diffusion des renseignements personnels (Politique de protection de la vie privée 3).

Cadre : L'accès aux outils de conformité et leur utilisation doivent être limités à un petit nombre de personnes autorisées seulement. 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 3).

9. SÉCURITÉ DU PERSONNEL

Politique 9a : Toutes les cours doivent s'assurer de disposer de procédures documentées pour l'orientation et les départs, et de programmes de formation continue pour les employés et les fournisseurs ayant accès à l'information judiciaire. Des processus doivent être mis en place pour confirmer que les employés et les fournisseurs disposent du 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 lors du départ ou de la transition à un nouveau rôle d'un employé ou d'un fournisseur.

Politique 9b : Nul ne devrait avoir accès à l'information judiciaire à moins de satisfaire au minimum aux conditions suivantes de la politique et d'avoir obtenu une autorisation de sécurité gouvernementale d'un niveau correspondant à son rôle.

Commentaire :

Avant d'obtenir l'accès à l'information judiciaire, l'utilisateur doit satisfaire au minimum aux conditions suivantes :

- besoin de savoir;
- avoir fait l'objet d'une vérification policière des antécédents de sécurité;
- avoir satisfait aux autres procédures applicables en matière de vérification de sécurité;
- 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 4);
- avoir reçu une formation sur l'ensemble des politiques, procédures et pratiques de sécurité applicables;
- avoir signé une entente documentant ses obligations en matière de sécurité de l'information judiciaire.

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

Cadre : 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 2).

10. CONTRÔLE D'ACCÈS

Politique 10a : Toutes les décisions de contrôle concernant l'information judiciaire relèvent de la responsabilité de la magistrature. Les utilisateurs devraient obtenir le niveau minimal d'accès requis pour leur rôle, conformément à leur niveau d'autorisation de sécurité. L'accès administrateur devrait être accordé de façon extrêmement limitée aux utilisateurs non judiciaires, uniquement pour le soutien administratif. Cet accès non judiciaire ne devrait être accordé qu'à la demande, puis être retiré lorsque son objectif immédiat est atteint.

Politique 10b : Les systèmes contenant de l'information judiciaire « personnelle » ou « individuelle » doivent être conservés dans un environnement adéquatement protégé, avec une surveillance accrue, des contrôles d'accès rigoureux et une protection par chiffrement, dans la mesure du possible. Les cours doivent établir une procédure d'ouverture de session sur tous les serveurs et dispositifs du réseau afin de détecter les tentatives d'accès non autorisé et les séquences d'opérations suspectes. Toute activité de ce type 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 l'agent de la sécurité informatique du système judiciaire.

Commentaire :

Cette politique ne tient pas pour acquis que la magistrature a le pouvoir exclusif de déterminer les rôles et les niveaux d'autorisation de sécurité; l'administration judiciaire doit aussi avoir le pouvoir de déterminer le niveau d'accès approprié pour les utilisateurs, parce que le personnel des cours a une responsabilité de reddition de compte double. Selon les principes généraux énoncés dans le Cadre de politique, cependant, l'administration judiciaire ne peut fournir à un utilisateur un niveau d'accès plus élevé que celui accepté par la magistrature.

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

Cadre : 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 5).

Cadre : L'information judiciaire doit être protégée contre l'accès non autorisé en conformité avec le Plan d'action du Conseil canadien de la magistrature en matière de sécurité des renseignements judiciaires (Politique de sécurité 1).

Cadre : 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 3).

11. SURVEILLANCE

Politique 11a : La 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 11b : L'application des outils d'analyse à l'information judiciaire (y compris l'information anonymisée) ne doit pas se faire sans l'avis et l'approbation de la magistrature.

Commentaire :

Bien que la surveillance du contenu, comme l'enregistrement de frappe, l'examen de l'historique de navigation sur le Web et la recherche automatisée par mot-clé des 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 de nature délicate et des renseignements permettant d'identifier une personne.[11] La recherche judiciaire peut nécessiter l'accès à des sites Web bloqués. Pour un modèle de politique d'utilisation acceptable, voir l'annexe 4 ci-dessous.

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

Cadre : Des évaluations de l'incidence sur la protection de la vie privée seront réalisées à l'étape de la conception de systèmes de gestion de l'information des cours qui tiennent compte de la collecte potentielle, de l'accès, de l'utilisation ou de la diffusion des renseignements personnels (Politique de protection de la vie privée 3).

12. GESTION DES APPAREILS MOBILES

Politique 12 : Les cours doivent se doter d'une politique conforme au Plan d'action pour les appareils mobiles et mettre en place des protocoles de sécurité prévoyant l'effacement des données des appareils perdus ou volés.[12]

Commentaire :

Qu'ils soient fournis par l'administration judiciaire, utilisés dans le cadre d'une politique sur l'utilisation des appareils personnels ou utilisés entièrement en dehors du programme de sécurité

[11] Voir ISO 27002, 12.4.1.

[12] Voir l'exemple de politique à l'annexe 3. Même avec des outils efficaces d'effacement à distance, si l'appareil n'est pas connecté à Internet ou s'il est placé en mode « avion », l'effacement à distance n'est pas possible.

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 c'est la tendance dominante, achetés par les utilisateurs, posent de nombreux risques pour la sécurité.

- Premièrement, les appareils mobiles peuvent être configurés pour accéder facilement et de partout aux ressources d'information en réseau. Cependant, et contrairement aux ordinateurs de bureau ou aux ordinateurs portables, qui sont achetés, fournis, configurés et entretenus par l'administration judiciaire, les appareils mobiles ne sont généralement pas conçus, ni construits ou configurés avec les mêmes capacités de sécurité.
- Deuxièmement, les appareils mobiles sont des ordinateurs qui peuvent générer, manipuler et conserver des données. Cependant, selon la configuration, la protection par mot de passe sur ces appareils peut être faible, les options de chiffrement limitées ou inexistantes, et les appareils peuvent être facilement égarés ou volés, donnant lieu à de graves transgressions de sécurité ou de protection de la vie privée.
- 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 immensément commode mais présente des risques importants, les données créées par l'utilisateur et les données concernant l'utilisateur étant transmises – souvent à l'insu de l'utilisateur – au tiers ayant créé le logiciel.
- Quatrièmement, les appareils mobiles sont branchés en permanence sur Internet et les capacités GPS intégrées leur permettent de suivre en temps réel la position et les activités de l'utilisateur. Si l'appareil est compromis, le microphone et la caméra intégrés peuvent aussi être utilisés pour enregistrer et transmettre des événements et des conversations sans que l'utilisateur ne le sache.

13. MÉDIAS SOCIAUX

Politique 13 : 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 médias et réseaux sociaux soulèvent de nombreuses questions auprès des tribunaux et de la magistrature, notamment en ce qui concerne la sécurité et la protection de la vie privée. Parmi celles-ci, mentionnons « les contrôles d'authentification insuffisants, l'injection de code indirect, la falsification de requête inter-site, l'hameçonnage, les fuites d'information, l'injection de code,

l'intégrité de l'information et l'anti-automatisation insuffisante ».[13] [Traduction] Les politiques et la formation devraient aborder tous les risques connus.

14. SIGNALEMENT ET GESTION DES INCIDENTS

Politique 14 : Chaque cour doit mettre en place un protocole pour le signalement des incidents de sécurité ayant trait aux utilisateurs judiciaires et à l'information judiciaire, 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 par la voie des canaux approuvés.

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 promptement l'incident à la ou aux personnes appropriées. Un processus de rapport d'incident comprend des mesures de sensibilisation et de formation pour tous les employés en ce qui concerne les mesures de sécurité, les signes avant-coureurs d'une infraction et les mécanismes de signalement appropriés.

Il faut inclure parmi les différents types d'atteintes à la sécurité la publication de dossiers de la cour faisant l'objet d'un interdit de publication ou avant leur publication approuvée par la cour.

Les Lignes de conduite sur la surveillance informatique (2002) du Conseil canadien de la magistrature précisent : « La surveillance informatique devrait être administrée par le personnel qui se rapporte directement au ou à la juge en chef de la Cour et qui relève directement de son autorité. » Ce principe devrait s'appliquer également au signalement d'incidents impliquant des utilisateurs judiciaires.

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

[13] Cité par Wu He, (2012), « A review of social media security risks and mitigation techniques », Journal of Systems and Information Technology, Vol. 14 iss : 2 pp. 171-180. (PDF), un examen des risques liés à la sécurité dans les médias sociaux et des techniques d'atténuation. Disponible sur : https://www.researchgate.net/publication/263528558_A_review_of_social_media_security_risks_and_mitigation_techniques [en anglais seulement].

15. CLASSIFICATION DES RENSEIGNEMENTS JUDICIAIRES

Politique 15a : Les cours devraient adopter un système de classification permettant l'identification des renseignements judiciaires sensibles afin de leur assurer une protection spéciale. Les systèmes de classification adoptés devraient être uniformes dans toutes les cours afin d'assurer une compréhension commune des exigences en matière de sensibilité et de protection des actifs.

Politique 15b : Aucun élément d'information judiciaire ne peut être publié, partagé, échangé ou fourni à un tiers, y compris à tout organisme gouvernemental, sans l'autorisation écrite préalable de la magistrature et conformément aux lois applicables.

Commentaire :

L'auteur d'un document devrait être responsable d'attribuer la classification qui convient aux renseignements qu'il a créés.

Le système de classification à deux paliers qui suit constitue un modèle très simple que les cours pourraient utiliser. D'autres approches peuvent être adoptées pour répondre aux besoins locaux, bien que l'uniformité d'une administration à l'autre serait préférable.

> **Renseignements réservés aux utilisateurs judiciaires** – Tous les renseignements judiciaires sont classifiés par défaut « réservés aux utilisateurs judiciaires » et par le fait même sont assujettis aux mesures de protection décrites dans le Plan d'action.
>
> **Renseignements protégés** – Cette classification peut être utilisée pour des renseignements judiciaires très sensibles, par exemple : des documents qui contiennent des renseignements personnels qui peuvent concerner les juges ou encore des litiges ou des parties, des projets de jugement, les courriels liés à un avis judiciaire et à la jurisprudence ainsi que les notes et mémoires portant sur des questions qui concernent la magistrature. Les renseignements protégés seraient sujets à un traitement plus rigoureux qui inclurait un étiquetage particulier, le chiffrement et l'entreposage sur des supports désignés.

L'auteur est responsable de décider quand les renseignements judiciaires ne sont plus classifiés et peuvent être divulgués à des utilisateurs non judiciaires. Par exemple, lorsque l'ébauche d'un jugement est finalisée, elle peut être rendue publique conformément aux instructions du juge.

Renvois : Gestion de l'actif, ISO 27001:2013, A.8.

16. CHIFFREMENT

Politique 16 : La magistrature doit participer à l'élaboration de la politique de chiffrement et à sa mise en œuvre, en ce qui concerne la confidentialité, l'intégrité, la non-répudiation et l'authentification des renseignements judiciaires. La politique et les procédures de chiffrement devraient être conformes au système de classification des renseignements judiciaires. Les activités principales de gestion, y compris les politiques et les procédures, doivent être confiées à la magistrature.

Commentaire :

L'objectif de cette politique est de rendre les outils de chiffrement facilement accessibles aux utilisateurs judiciaires, de gérer le processus de chiffrement de façon sécuritaire et de protéger les renseignements de nature délicate contre tout accès non autorisé.

Les logiciels, les normes et les protocoles de gestion relatifs au chiffrement des données au moyen de certificats numériques comprennent ce qu'on appelle l'ICP, ou l'infrastructure à clé publique.

Un certificat numérique, émis par un tiers de confiance, vérifie l'identité d'un utilisateur et le connecte à une clé publique unique, ce qui permet l'échange et le déchiffrement de messages chiffrés. Pour assurer une indépendance totale, il est recommandé que le pouvoir de certification des utilisateurs judiciaires soit assumé par un tiers de confiance indépendant non seulement de la magistrature, mais aussi du gouvernement.

La décision de chiffrer les données devrait être fondée sur des décisions documentées de gestion des risques pour la sécurité des tribunaux et sur l'application du système de classification des renseignements judiciaires.

• Quiconque utilise le chiffrement des renseignements judiciaires doit être connu de la magistrature et fournir des renseignements sur la fonctionnalité du produit.

• L'ASISJ devrait enseigner à tous les utilisateurs comment se servir de la technologie de chiffrement et élaborer et documenter des procédures de récupération de l'information chiffrée. Il devrait également être chargé de surveiller toutes les demandes d'authentification des utilisateurs.

Renvois : ISO 27001:2013A.10. ISO 27017:2015, art. 10, ISO 27002, 10.1.

17. SÉCURITÉ MATÉRIELLE

Politique 17 : L'ensemble de l'équipement et des installations utilisés dans le traitement de l'information judiciaire doit être situé dans un lieu physiquement sécurisé, dont l'accès est limité aux personnes autorisées. Les mesures de sécurité matérielle 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 matérielle renvoie à la protection des bâtiments et de l'équipement (ainsi que de l'information et des logiciels qui y sont contenus) contre l'intrusion par effraction, le vol, le vandalisme, les catastrophes naturelles ou artificielles et les dommages accidentels. Les gestionnaires doivent s'intéresser à la construction de centres de traitement de données, à l'affectation des salles, aux procédures de mesures d'urgence, aux règlements qui régissent la disposition et l'utilisation de l'équipement, à l'alimentation en énergie et en eau, à la manutention des produits et aux relations avec le personnel, les entrepreneurs externes, les autres cours ainsi que les ministères, organismes et tribunaux gouvernementaux. Ces mesures s'appliquent, que l'équipement se trouve ou non dans les locaux.

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

18. SYSTÈMES D'INFORMATION

Politique 18 : Les processus d'acquisition, de développement et de maintenance des systèmes d'information de la cour doivent être conçus et appliqués afin de préserver la qualité, l'intégrité et la disponibilité à long terme de l'information judiciaire et de l'information de la cour. L'information judiciaire doit faire l'objet d'une protection additionnelle au-delà des mesures de sécurité applicables à l'information de la cour.

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

Cadre de politique : Politique fondamentale 10, Politique de sécurité 5.

19. COMMUNICATIONS ET EXPLOITATION

Politique 19a : Les programmes de sécurité judiciaire doivent comprendre des contrôles, des procédures et des pratiques documentés et approuvés en matière d'exploitation, et 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 ou de technologie de communication.

Politique 19b : Il incombe aux cours 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 en exploitation
10. Installation de logiciels sur des systèmes en exploitation
11. Gestion des vulnérabilités techniques
12. Restrictions liées à l'installation de logiciels
13. Mesures relatives à l'audit des systèmes d'information

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

Cadre de politique : Les cours doivent mettre en place et tenir à jour des pratiques exemplaires pour la sécurisation des réseaux locaux sans fil (RL sans fil) et s'assurer que les utilisateurs ne compromettent pas la sécurité de l'information judiciaire lorsqu'ils utilisent les réseaux sans fil. (« 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 6).

Cadre de politique : Les systèmes et les technologies d'information des cours doivent 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 4).

20. CONTINUITÉ DES ACTIVITÉS

Politique 20 : Les cours doivent protéger l'information judiciaire en cas de catastrophe ou d'autres défaillances du système, et fournir un degré élevé d'assurance que toute perturbation du service résultant d'un tel événement sera la plus brève possible. Les utilisateurs judiciaires doivent avoir accès au stockage réseau et le contenu de celui-ci doit être sauvegardé au moins une fois par jour. Des dispositions efficaces doivent être prises en vue de faciliter la sauvegarde des renseignements judiciaires créés ou reçus (si stockés localement), par exemple sur des appareils mobiles.

Commentaire :

Un plan de continuité des activités doit être préparé en s'appuyant sur l'évaluation des menaces et des risques et devrait inclure un processus de mise à jour. Tous les plans de continuité des activités doivent être conformes au Plan d'action et comprendre au moins les éléments suivants :[14]

1 Gouvernance
2 Analyse des effets sur les activités
3 Plans, mesures et arrangements pour la continuité des activités
4 Procédures 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.

PRINCIPAUX RENVOIS

Le Cadre de politique offre une approche fondée sur des principes permettant d'établir un large éventail de politiques d'information judiciaire, notamment la sécurité de l'information. L'un des aspects du mandat de mise à jour du Plan d'action consiste donc à assurer la cohérence avec les valeurs, les principes, les politiques et les définitions énoncés dans le Cadre de politique, auquel le lecteur du Plan d'action devrait se référer.[15]

Sauf indication contraire, les renvois mentionnés dans chaque section de la politique sont les trois documents suivants :

- ISO/CEI 27001 et 27002:2013

[14] Pour un guide de base, voir https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-fr.aspx, « Guide de planification de la continuité des activités », Sécurité publique Canada.
[15] https://www.cjc-ccm.gc.ca/cmslib/general/AJC/Information%20Judiciaire%20dans%20le%20monde%20num%C3%A9rique%202013-03.pdf

- Security and Privacy Controls for Information Systems and Organizations, NIST Special Publications SP800-53r5 [en anglais seulement]

Parmi les normes choisies pour les administrations canadiennes, mentionnons :

- British Columbia Information Security Policy (juillet 2016) publié par le Bureau du dirigeant principal de l'information du gouvernement [en anglais seulement]
- NTI-GO - Gouvernement de l'Ontario (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)
- Standard of Good Practice for Information Security (2016), publiée par l'Information Security Forum (ISF) et utilisée au Nouveau-Brunswick [en anglais seulement]
- Gestion des risques liés aux TI (voir https://www.cse-cst.gc.ca/fr/publication/list/IT-Risk-Management)
- ITSB-67 - Facteurs de cybersécurité à considérer par la direction - Conseils à l'intention du gouvernement du Canada
- ITSE.10.033 Gestion des risques liés à la Sécurité des TI au sein du gouvernement du Canada
- Nuage (voir https://www.cse-cst.gc.ca/fr/publication/list/Cloud)
- ITSE.50.060 Sécurité infonuagique pour le Gouvernement du Canada
- ITSB-105 Recours à des services contractuels d'infonuagique publique : implications sur le plan de la sécurité

ANNEXE 1

RECOMMANDATIONS DU CCT APPROUVÉES PAR LE CONSEIL LE 30 NOVEMBRE 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 l'utilisation des nouvelles technologies par les juges).

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 Bureau du commissaire 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 de la fonction 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 faire la priorité à la sécurité du système d'information des cours;

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

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

   d) de faire en sorte qu'un membre du personnel en technologies de l'information relevant du juge en chef soit nommé à la gestion de 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 document provisoire englobant toutes les mesures de sécurité recommandées pour toutes les cours canadiennes et fasse en sorte que le Comité dispose des ressources nécessaires à cette fin.

ANNEXE 2

GLOSSAIRE DE TERMES ET D'ACRONYMES DÉFINIS

Terme ou acronyme	Sens
Analytique	« L'application de l'informatique, de la recherche opérationnelle et de la statistique à la résolution de problèmes » - voir Voir http://fr.wikipedia.org/wiki/Analytique_(recherche).
Anonymisation	Le processus par lequel les renseignements personnels sont retirés des ensembles de données.
Apps	Applications logicielles téléchargées pour utilisation sur des appareils mobiles.
Mégadonnées	Définition courante : un volume de données tel qu'il est impossible de les traiter sans outils logiciels spécialisés. On trouvera une bonne explication ici : http://www-01.ibm.com/software/data/bigdata/.
PAP	Abréviation de l'expression « Prenez vos appareils personnels », une politique qui permet aux employés d'accéder aux réseaux d'affaires à partir d'appareils mobiles qui sont leur propriété personnelle.
Nuage	« L'informatique en nuage est un modèle permettant un accès systématique, commode et à la demande à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) pouvant être fournies et libérées rapidement avec un minimum d'effort de gestion et d'interaction avec le fournisseur de service. » Traduit de NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
Cryptographie	La science du chiffrement.
FSN	Fournisseur de services en nuage.
DDoS	Déni de service distribué; type de cyberattaque évolué qui surcharge un site Web et empêche les utilisateurs d'y accéder.
Chiffrement	Transformation d'un texte lisible par l'utilisateur en code illisible afin de protéger l'information de l'accès non autorisé.
Pare-feu	Un produit matériel ou un logiciel programmé pour filtrer les intrusions non désirées d'un ordinateur ou d'un réseau à un autre.
IDS	Système de détection d'intrusion – système qui surveille les tentatives d'accès non autorisées à un réseau.
Intrusion	L'intrusion est définie comme une tentative visant à compromettre la sécurité d'un ordinateur ou d'un réseau. La détection d'intrusion est le processus qui consiste à surveiller les évènements qui surviennent dans le système informatique ou dans le

Terme ou acronyme	Sens
	réseau et à les analyser pour détecter des signes d'intrusions.
FAI	Fournisseur d'accès Internet – organisme qui fournit l'accès à l'Internet.
RL	Réseau local – système qui relie des utilisateurs à des ressources informatiques partagées à l'intérieur d'un immeuble.
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 regroupant les virus et vers informatiques, les logiciels-espions, les chevaux de Troie, les maliciels, les attaques de déni de service, etc.
Sécurité matérielle	La sécurité matérielle s'entend de la protection des immeubles et de l'équipement (ainsi que des renseignements et logiciels qui s'y trouvent) des introductions par effraction, vols, actes de vandalisme, catastrophes naturelles et autres et dommages accidentels.
Services partagés	L'expression services partagés renvoie à la prestation de services par un groupe au sein de l'organisme, lorsque ces services étaient auparavant assurés par plus d'un groupe au sein de l'organisation. Le financement et le ressourcement des services sont partagés et le groupe qui les fournit devient à toutes fins utiles un fournisseur de services interne. Traduit de Wikipedia, http://en.wikipedia.org/wiki/Shared_services.
ENS	Entente de niveau de service. L'ENS cristallise la compréhension des parties sur les services, les priorités, les responsabilités et les garanties. Chaque partie de la portée des services doit faire l'objet d'un « niveau de service » précis. L'ENS peut préciser le degré de disponibilité, la serviabilité, le rendement, l'exploitation ou autres attributs du service, comme la facturation. Traduit de Wikipedia, http://en.wikipedia.org/wiki/Service-level_agreement.
EMR	Évaluation des menaces et des risques.
Virtualisation	« La virtualisation consiste à faire fonctionner un ou plusieurs systèmes d'exploitation ou applications comme un simple logiciel, sur un ou plusieurs ordinateurs, serveurs ou système d'exploitation, au lieu de ne pouvoir en installer qu'un seul par machine. Grâce à la virtualisation, une entreprise peut gérer plus facilement les mises à jour et les modifications du système d'exploitation et des applications sans nuire à l'utilisateur. » Traduit de Wikipedia, http://en.wikipedia.org/wiki/Virtualization.
WiFi	Utilisé de façon interchangeable avec RL sans fil, bien que techniquement, il s'agisse d'un RL sans fil configuré selon une norme particulière.
RL sans fil	Réseau local qui fonctionne par radiofréquence au lieu d'être branché au moyen de câbles.

ANNEXE 3

EXEMPLE DE POLITIQUE DE SÉCURITÉ DES APPAREILS MOBILES DE SOPHOS

Traduit sans modifications depuis http://www.sophos.com/en-us/medialibrary/PDFs/other/Example%20Mobile%20Device%20Security%20Policy.docx.

Exemple de politique de sécurité des appareils mobiles

Utilisation de la politique

L'un des défis auxquels sont confrontés les services de TI aujourd'hui porte sur la sécurisation des appareils mobiles appartenant aux individus et à l'organisme, comme les téléphones intelligents et les tablettes informatiques. Cet exemple de politique vise à servir de guide pour les organismes qui souhaitent mettre à jour leur politique de sécurité des appareils mobiles ou en adopter une.

N'hésitez pas à l'adapter à votre organisme. Au besoin, modifiez, retirez ou ajoutez des éléments en fonction de vos besoins et de votre attitude à l'égard du risque. Il ne s'agit pas d'une politique complète, mais d'un modèle pragmatique destiné à servir de base pour l'élaboration de votre propre politique.

Contexte de la politique

Le principal défi vient du fait que les utilisateurs ne reconnaissent pas que les appareils mobiles représentent une menace pour la sécurité des TI et des données. Pour cette raison, ils n'appliquent souvent pas les mêmes lignes directrices en matière de sécurité et de protection des données qu'ils appliquent sur d'autres appareils, comme les ordinateurs personnels.

Le second défi vient du fait que les utilisateurs, lorsqu'ils fournissent leur propre appareil, sont souvent plus portés à donner plus de poids à leurs droits sur l'appareil qu'au besoin de l'employeur de protéger les données.

Ce modèle de politique fournit un cadre pour la sécurisation des appareils mobiles et devrait être rattaché aux autres politiques qui appuient la position de votre organisme en matière de sécurité des TI et des données.

Exemple de politique

1. Introduction

Les appareils mobiles, comme les téléphones intelligents et les tablettes informatiques, sont des outils importants pour leur organisation et leur utilisation est appuyée pour atteindre les objectifs de l'organisation.

Cependant, les appareils mobiles représentent aussi un risque important pour la sécurité de l'information et des données puisqu'ils peuvent constituer une voie d'accès non autorisé à l'infrastructure de données et de TI de l'organisme si les applications et les procédures de sécurité ne sont pas appliquées. Ceci peut ensuite conduire à des pertes de données et à une infection du système.

<Nom de l'organisme> doit protéger ses actifs d'information afin de protéger ses clients, ses propriétés intellectuelles et sa réputation. Ce document donne les grandes lignes d'un ensemble de pratiques et d'exigences pour l'utilisation sécuritaire des appareils mobiles.

2. Portée

1. Tous les appareils mobiles, qu'ils soient la propriété de <Nom de l'organisme> ou de ses employés, qui ont accès aux réseaux, aux données et aux systèmes de l'organisation, à l'exclusion des ordinateurs mobiles gérés par les services de TI de l'organisme. Ceci comprend les téléphones intelligents et les tablettes informatiques.

2. Exemptions : lorsqu'il existe un motif opérationnel d'exclure un appareil de l'application de la politique (trop coûteux, trop complexe, répercussions négatives sur les autres exigences opérationnelles), une évaluation des risques doit être effectuée avec l'autorisation de la direction de la sécurité.

3. Politique

3.1 Exigences techniques

1. Les dispositifs doivent utiliser l'un des systèmes d'exploitation suivants : Android 2.2 ou plus récent, IOS 4.x ou plus récent. <ajouter ou retirer au besoin>.
2. Les appareils doivent conserver tous les mots de passe sauvegardés par l'utilisateur dans un répertoire chiffré.
3. Les appareils doivent être configurés avec un mot de passe sûr, conforme à la politique sur les mots de passe de <Nom de l'organisme>. Ce mot de passe ne doit pas reprendre tout autre authentifiant utilisé au sein de l'organisme.
4. À l'exception des appareils sous la gestion des TI, aucun appareil ne peut être branché directement au réseau interne de l'organisme.

3.2 Exigences relatives aux utilisateurs

1. Les utilisateurs ne doivent charger dans leurs appareils mobiles que les données essentielles à l'exécution de leurs fonctions.
2. Les utilisateurs doivent signaler sans délai le vol ou la perte de leurs appareils mobiles aux services de TI de <Nom de l'organisme>.
3. Si un utilisateur a des raisons de croire qu'un accès non autorisé aux données de l'organisation a pu avoir lieu à partir d'un appareil mobile, l'utilisateur doit signaler l'incident conformément au processus de signalement des incidents de <Nom de l'organisme>.
4. Les appareils ne doivent pas être « déverrouillés » et on ne doit pas y installer de logiciel ou de micrologiciels conçus pour donner accès à des fonctionnalités qui ne sont pas destinées à être portées à la connaissance de l'utilisateur.
5. Les utilisateurs ne doivent pas installer de logiciels piratés ou de contenu illégal dans leurs appareils.
6. Les applications ne doivent être installées qu'à partir de sources officiellement approuvées par le propriétaire de la plateforme. L'installation de code provenant de sources non sécurisées est interdite. Si vous n'êtes pas certain que l'application provient d'une source approuvée, veuillez communiquer avec les TI de <Nom de l'organisme>.
7. Les appareils doivent être tenus à jour avec les rustines fournies par le fabricant ou le réseau. Au minimum, l'utilisateur doit vérifier l'émission de rustine au moins toutes les semaines et appliquées une fois par mois.
8. Les appareils ne doivent pas être branchés à un ordinateur qui n'est pas doté d'une protection anti-maliciel à jour et conforme à la politique de l'organisme
9. Les appareils doivent être chiffrés selon les normes de conformité de <Nom de l'organisme>.
10. Les utilisateurs doivent faire preuve de prudence s'ils utilisent des comptes personnels et d'affaires sur leurs appareils. Ils doivent tout particulièrement veiller à ce que les données de l'organisme ne soient transmises que par l'entremise du système de courriel de l'organisme. Si un utilisateur soupçonne que des données de l'organisation ont pu être transmises via un compte de courriel personnel, dans le texte ou en pièce jointe, il doit en aviser immédiatement les TI de <Nom de l'organisme>.
11. (Si applicable à votre organisation) Les utilisateurs ne doivent pas utiliser les postes de travail de l'organisme pour sauvegarder ou synchroniser du contenu comme des fichiers médias, à moins que ce contenu ne soit requis pour des motifs professionnels légitimes.

*Le déverrouillage d'un appareil signifie en retirer les limites imposées par le fabricant. Ceci donne accès au système d'exploitation, ce qui en déverrouille toutes les caractéristiques et permet l'installation de logiciels non autorisés.

ANNEXE 4

MODÈLE DE POLITIQUE D'UTILISATION ACCEPTABLE

Le Conseil canadien de la magistrature a rédigé la présente politique d'utilisation acceptable pour servir de modèle auprès des cours. Toute politique concernant l'utilisation acceptable chez les utilisateurs judiciaires doit tenir compte des principes d'indépendance (institutionnelle et individuelle) et des enjeux suivants :

1. Qui établit les règles?
2. Qui décide des exceptions?
3. Comment assure-t-on la surveillance des comportements et de la conformité?
4. Comment enquête-t-on sur la violation de la politique et comment signale-t-on les violations?
5. Comment gère-t-on les cas de non-conformité?

Objet : Veiller à ce que les utilisateurs judiciaires aient un accès ininterrompu à un système d'information sécurisé, privé et fiable (le « service »). La politique doit se conformer aux principes de l'indépendance judiciaire et aux Lignes de conduite sur la surveillance informatique du Conseil.

Les activités suivantes sont généralement interdites à tous les utilisateurs :

- Utiliser le service pour exploiter une entreprise privée.
- Tenter d'accéder au compte d'un autre utilisateur.
- Partager des mots de passe.
- Revendre le service à un tiers.
- Envoyer un courriel de masse non sollicité.
- Accéder aux sites Web bloqués*.
- Télécharger ou installer des logiciels non approuvés*.
- Surcharger le service (ou les réseaux connectés au service)*.
- Adopter, faciliter ou favoriser un comportement illégal.
- Endommager, désactiver ou entraver le service.
- Interférer avec l'utilisation et la jouissance du service par une autre personne.

***Exceptions.** Il arrive de temps à autre qu'un utilisateur judiciaire doive avoir accès à un site Web bloqué, doive installer des logiciels non approuvés pour des motifs opérationnels légitimes, ou doive télécharger ou diffuser des volumes de données exceptionnellement élevés. Dans ces cas, le [fournisseur de services] doit disposer d'un processus de traitement des demandes de dérogation et d'approbation raisonnable d'une solution de rechange pour répondre au besoin.

Surveillance et intervention en cas d'incident. Le [fournisseur de services] a le droit de surveiller l'activité des utilisateurs et du réseau afin de protéger tous les utilisateurs contre les activités non autorisées. Toutefois, conformément aux Lignes de conduite sur la surveillance informatique, « 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. »

Lorsque le [fournisseur de services] a des motifs de croire qu'un utilisateur judiciaire s'est livré à une activité non autorisée, il lui incombe de communiquer sans délai ses constatations à la magistrature avant de prendre toute autre mesure.

Suspension. En consultation avec l'ASISJ, le [fournisseur de services] peut suspendre l'accès d'un utilisateur judiciaire au service si :

(1) le service est utilisé à des fins non autorisées;

(2) le service est utilisé à des fins criminelles ou illégales.

Réintégration. Un utilisateur peut être réintégré après consultation entre la magistrature et [le fournisseur de services].