



Conseil canadien de la magistrature

LIGNES DIRECTRICES  
SUR LA MIGRATION  
DE L'INFORMATION JUDICIAIRE  
VERS UN FOURNISSEUR DE  
SERVICES D'INFORMATIQUE EN NUAGE

Préparé par le D<sup>r</sup> Martin Felsky, PhD, JD  
Conseiller spécial du CCM en technologie de l'information

Septembre 2019

## TABLE DES MATIÈRES

Contexte .....	3
[1] Conditions préalables .....	3
[a] L'évaluation des menaces et des risques .....	3
[b] L'évaluation des facteurs relatifs à la vie privée (EFVP) .....	4
[c] La définition d'information judiciaire .....	4
[d] La définition d'utilisateurs judiciaires .....	5
[e] La classification de l'information judiciaire .....	5
[f] Le lieu de résidence de l'information .....	5
[g] La gestion des documents .....	6
[h] La formation .....	6
[2] L'indépendance .....	6
[3] Autres questions de sécurité et de confidentialité .....	7
[4] Le niveau de service et la fonctionnalité .....	8

## CONTEXTE

La perspective de la migration vers l'informatique en nuage soulève plusieurs préoccupations parmi la magistrature.<sup>1</sup> Les présentes lignes directrices ont été élaborées à la demande du Sous-comité de la technologie du Conseil, afin d'aider les juges de l'ensemble du Canada à déterminer s'ils devraient migrer vers l'informatique en nuage avec leurs administrations respectives et, si oui, dans quelles circonstances. Les lignes directrices sont divisées en quatre grandes sections :

1. Les conditions préalables
2. L'indépendance
3. Autres questions de sécurité et de confidentialité
4. Le niveau de service et la fonctionnalité

Dans chaque section on indique si la ligne directrice est « nécessaire » ou « souhaitable ».

## [1] CONDITIONS PRÉALABLES

**Les activités que la magistrature doit entreprendre avant de migrer vers l'information en nuage. Elles sont considérées comme étant « nécessaires ».**

### [A] L'ÉVALUATION DES MENACES ET DES RISQUES

Avant de transférer de l'information confidentielle au nuage informatique, une évaluation des menaces et des risques (EMR) devrait être effectuée. Afin de pouvoir confier l'information judiciaire à un système informatique quelconque, il est essentiel d'en comprendre les risques. L'évaluation des menaces et des risques sert de base à la classification de l'information selon les niveaux de protection appropriés. Les politiques en matière de sécurité sont fondées sur les résultats d'une évaluation des menaces et des risques.

La *Méthodologie harmonisée d'EMR (TRA-1)*, établie par le Centre canadien de réponse aux incidents cybernétiques (qui fait maintenant partie du Centre canadien pour la cybersécurité), est un modèle uniformisé qui est utile non seulement pour faire une évaluation EMR, mais aussi pour rédiger un énoncé des travaux pour services de consultants en EMR.

Voir <https://cyber.gc.ca/fr/orientation/methodologie-harmonisee-demr-tra-1>.

Il existe d'autres modèles d'EMR. Les tribunaux peuvent choisir de suivre tout modèle qui convient à leur situation. Par exemple, voir le document intitulé *Threat Risk Assessment Template* (2018), disponible en anglais seulement, et produit par le gouvernement de la Saskatchewan.

Voir <https://taskroom.sp.saskatchewan.ca/Documents/Threat-Risk-Assessment-Template.pdf>

---

<sup>1</sup> Pour un examen plus complet de la question, voir « *L'information judiciaire dans le nuage informatique : les arguments en faveur de l'indépendance* », produit par Martin Felsky pour le Conseil canadien de la magistrature, 21 août 2018.

## [B] L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

Avant de transférer de l'information à un nouveau système, une évaluation devrait être effectuée pour déterminer si elle contient des renseignements personnels qui pourraient être assujettis aux lois sur la protection de la vie privée et l'accès à l'information, et pour savoir comment répondre aux exigences en matière de protection, de consentement, d'accès, de conservation et autres.

Selon le Commissariat à la protection de la vie privée du Canada (CPVP), les étapes habituelles d'une EFVP sont les suivantes :<sup>2</sup>

- Repérer tous les renseignements personnels concernant un programme ou un service, et examiner la façon dont ils seront utilisés;
- Appliquer le critère en quatre parties du CPVP pour la nécessité et la proportionnalité des initiatives ou des technologies hautement intrusives (pour plus d'information, voir le document *Nos attentes* du CPVP : [https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/gd\\_exp\\_201103/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/gd_exp_201103/));
- Appliquer les dix principes régissant la protection des renseignements personnels;
- Déterminer où les renseignements personnels sont envoyés après leur collecte;
- Déceler les risques d'entrave à la protection de la vie privée et évaluer leur niveau;
- Trouver des façons d'éliminer ou de réduire les risques d'entrave à la vie privée à un niveau acceptable.

Tout comme l'EMR, l'évaluation des facteurs relatifs à la vie privée peut être faite selon un modèle qui convient à la juridiction. Par exemple, voir le modèle d'EFVP du gouvernement de la Nouvelle-Écosse qui est disponible en anglais seulement

: <https://novascotia.ca/just/IAP/docs/Appendix%20B%20PIA%20Template.pdf>.

Voir aussi la *Directive sur l'évaluation des facteurs relatifs à la vie privée* du gouvernement du Canada : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308>.

## [C] LA DÉFINITION D'INFORMATION JUDICIAIRE

L'information judiciaire doit être définie et différenciée par rapport à d'autres genres d'information, par exemple l'information des tribunaux ou les renseignements personnels des juges.

La migration vers l'informatique en nuage soulève une question fondamentale : que migre-t-on exactement? La migration la plus simple est généralement vers un système de courriel et un dépôt de documents hébergés (par exemple, Microsoft Outlook et OneDrive ou SharePoint). La magistrature doit

---

<sup>2</sup> Commissariat à la protection de la vie privée du Canada, [https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/02\\_05\\_d\\_33/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/02_05_d_33/).

définir quelle information lui appartient exclusivement, par rapport aux documents des tribunaux ou à l'information concernant l'administration des tribunaux, par exemple.

## [D] LA DÉFINITION D'UTILISATEURS JUDICIAIRES

1. Pour les besoins d'accès et d'autorisation, déterminer qui sont les « utilisateurs judiciaires » et quel niveau d'autorisation est nécessaire à l'exercice de leurs fonctions.
2. Établir un processus pour ajouter, supprimer et autoriser des utilisateurs judiciaires, et élaborer une politique concernant l'accès par des tiers (s'il en est).
3. Élaborer et adopter des exigences en matière d'autorisation de sécurité applicables à toute personne ayant accès aux serveurs physiques.

Il est recommandé que la définition d'information judiciaire et celle d'utilisateurs judiciaires soient uniformisées autant que possible parmi l'ensemble des tribunaux. L'uniformité de ces définitions rendra la migration vers l'informatique en nuage et la gestion de l'information dans le nuage plus simple et moins coûteux. La principale référence à ce sujet est le document de travail du Conseil canadien de la magistrature intitulé *Cadre de politique de gestion de l'information judiciaire dans le monde numérique* (2013) : <http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Information%20Judiciaire%20dans%20le%20monde%20numérique%202013-03.pdf>.

Un sommaire des principaux points de ce document de 69 pages se rapportant à ces définitions est disponible à l'annexe 2A de ce document (pages 69 à 71). Le document propose des modèles pour aider les tribunaux à formuler les définitions.

Deux documents utiles issus du projet de système d'information judiciaire des tribunaux de la Nouvelle-Écosse sont également joints (aux annexes A et B), à titre d'exemples de modèles concrets. Ils sont disponibles en anglais seulement.

## [E] LA CLASSIFICATION DE L'INFORMATION JUDICIAIRE

L'information judiciaire doit être classifiée selon son niveau de confidentialité.

Toute l'information judiciaire – telle qu'elle est définie – n'exige pas nécessairement le même niveau de protection. Le *Plan d'action en matière de sécurité des renseignements judiciaires* recommande que l'information judiciaire soit classifiée selon son niveau de confidentialité, d'après les résultats de l'évaluation des menaces et des risques.

## [F] LE LIEU DE RÉSIDENCE DE L'INFORMATION

Le lieu de résidence de l'information (y compris OneDrive et SharePoint) doit demeurer au Canada (lorsque l'information est immobile ou en transit, y compris les copies de sauvegarde). Lorsque l'information est en transit, cette dernière devrait demeurer au Canada, lorsque possible.

## [G] LA GESTION DES DOCUMENTS

1. La magistrature doit décider comment éliminer l'information judiciaire stockée dans le nuage informatique, lorsque des fichiers sont supprimés ou qu'un utilisateur prend sa retraite.
2. La magistrature doit décider si le nuage informatique peut servir à archiver l'information judiciaire à long terme.
3. La magistrature doit avoir un plan pour la fin d'un contrat d'hébergement et le transfert méthodique de l'information à un autre hôte.

## [H] LA FORMATION

Malgré la plus solide infrastructure de sécurité et la meilleure technologie de cryptage, la plupart des atteintes à la sécurité sont dues au comportement des utilisateurs. C'est pourquoi une formation complète et continue sur la sécurité de l'information doit être offerte à l'ensemble des utilisateurs de tout système contenant de l'information judiciaire.

## [2] L'INDÉPENDANCE

**Tous ces éléments sont « nécessaires » – sauf indication contraire ci-dessous.**

1. Le recours au même fournisseur de services d'informatique en nuage faciliterait la migration vers un nuage communautaire pour les juges dans l'avenir.
2. Il pourrait être préférable que les utilisateurs judiciaires soient un locataire unique, plutôt que d'être en colocation.
3. Les utilisateurs judiciaires devraient avoir leur propre domaine de courriel.
4. Les modalités contractuelles doivent être mises à la disposition des juges.
5. Les conflits potentiels entre Microsoft et les politiques judiciaires doivent être résolus.
6. Cryptage de bout en bout à clé double (par défaut), la seconde clé étant contrôlée par la magistrature.
7. Le message à l'écran de connexion ne peut être personnalisé – le gouvernement devrait donc ajouter un avis de non-responsabilité à l'intention des utilisateurs judiciaires.
8. Le fournisseur de services d'informatique en nuage doit observer des politiques précises concernant la notification d'une atteinte à la sécurité ou à la vie privée (voir aussi la section Autres questions de sécurité et de confidentialité).
9. La magistrature peut élaborer des politiques de sécurité applicables aux appareils personnels utilisés pour obtenir accès à l'information confidentielle.

### [3] AUTRES QUESTIONS DE SÉCURITÉ ET DE CONFIDENTIALITÉ

**Ces éléments correspondent tous aux exigences du *Plan d'action en matière de sécurité des renseignements judiciaires* et doivent donc être considérés comme étant « nécessaires ».**

1. Déterminer la limite du niveau de confidentialité de l'information que le fournisseur est disposé à héberger. (Par exemple, Services partagés Canada offre des services d'informatique en nuage seulement pour l'information non classifiée.)
2. Le fournisseur de services d'informatique en nuage doit observer des politiques précises concernant la notification d'une atteinte à la sécurité ou à la vie privée (voir aussi la section sur L'indépendance).
3. Le fournisseur de services d'informatique en nuage doit offrir une redondance (y compris des liens de réseau redondants) et un déclenchement rapide de la reprise (continuité des activités) (voir aussi la section sur Le niveau de service et la fonctionnalité).
4. Cryptage par l'utilisateur final avec formation.
5. Les utilisateurs peuvent voir qui a tenté d'obtenir accès à un document crypté (et qui a réussi à le faire).
6. Les utilisateurs peuvent limiter les destinataires autorisés à lire, à modifier, à imprimer ou à acheminer un courriel ou un document.
7. Mesures pour prévenir l'accès non autorisé.
8. Registres d'accès privilégié accessibles à la magistrature.
9. Mesures de protection de cybersécurité offertes en tout temps (24/7).
10. Accès administrateur restreint.
11. Vérification de l'accès administrateur privilégié aux utilisateurs et à l'information judiciaire, avec alertes.
12. Authentification à facteurs multiples.
13. L'hôte doit effectuer des essais de pénétration.
14. Le fournisseur de services d'informatique en nuage doit sauvegarder les données.
15. L'hôte doit avoir un plan de reprise après sinistre.
16. L'hôte doit avoir une stratégie et un processus de surveillance de réseau pour surveiller le trafic du réseau. (voir aussi la section sur L'indépendance)
17. Conformité au *Plan d'action en matière de sécurité des renseignements judiciaires* et aux normes de sécurité internationales.
18. Vérifications de sécurité périodiques effectuées par un tiers.

19. La magistrature peut élaborer des politiques de sécurité applicables aux appareils personnels utilisés pour obtenir accès à l'information confidentielle. (voir aussi la section sur L'indépendance)

## [4] LE NIVEAU DE SERVICE ET LA FONCTIONNALITÉ

**Que ces éléments soient nécessaires ou souhaitables, ils peuvent être négociés selon les préférences locales.**

1. Interopérabilité avec les systèmes des tribunaux (peut entrer en conflit avec l'indépendance judiciaire, dans une certaine mesure).
2. Il doit y avoir un accord sur les niveaux de service qui indique le temps de réponse du fournisseur de services d'informatique en nuage.
3. L'hôte doit offrir un service d'assistance dont les heures de disponibilité sont convenables.
4. Disponibilité à 99,9 % sans temps d'arrêt prévu.
5. Le fournisseur de services d'informatique en nuage doit offrir une redondance (y compris des liens de réseau redondants) et un déclenchement rapide de la reprise (continuité des activités) (voir aussi la section Autres questions de sécurité et de confidentialité)
6. L'hôte doit avoir un plan de communication pour aviser les utilisateurs des arrêts de service prévus et des pannes imprévues.



# ANNEXE A

Information gathered, produced or used for judicial purposes  (as discussed at our meeting on May 24 and , in this column, limited to that related directly to a judge)	Access	Others who gather, produce, use document/s listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
Information relating to private or personal affairs and social interactions of a judge	J, JA with J consent	Scheduling and backup, CJ, ACJs, EAs	NNSC- ACJ PC/FC- CJ	Diary, calendar		Google calendar, iPad, iPhone		CIS (perhaps not specific details but block of time) Outlook	BES (for Blackberry users)
Work relating to a <i>Case File</i> that is highly sensitive in nature (e.g. draft judgments, working notes, digital dictations, etc.)	J, JA , Law Clerk with consent**			√	I,C,F	√			
Audit logs containing summaries of computer system activities undertaken by a judge	O, without J permission	JITSO CIO	JITSO, CIO With CJ Consent (in accordance with CJC Monitoring Guidelines)		C	√	Printer job history may include dates, times, file names	FileNet, applications (CIS, JEIN) log certain activities NOVO?	Server(s), Databases
History of web sites visited by a judge	O, without CJ permission	JITSO CIO staff/admins	JITSO w CJ Consent		C			√	√
All sms (Text) and voice messages***	J, with J consent	Recipients				√		Phone	BES
Diary and calendar events other than docket	J, with J consent	NSSC: All J's have access to		√	Word P'cess	√	√	JEIN, CIS??	BES, Smartphones

Information gathered, produced or used for judicial purposes  (as discussed at our meeting on May 24 and , in this column, limited to that related directly to a judge)	Access	Others who gather, produce, use document/s listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
events that directly relate to a <i>Case File</i>		calendar; Scheduler, CJ, ACJ;PC: Master diary							
Contact details :address book information held on cell phones or in desktop software app or other electronic repositories	J, with J consent	Anyone with J consent		√	√	√	√	Judicom, Outlook	BES
Social networking information that is not in the public domain, for example private blogs or closed collaborative networks used by judges and their professional colleagues	J							CAPCJ Judicom/JAIN (Note: Not in NS gov)	
Information regarding the scheduling of judges within a court calendar. CA Panel selection process?	J, JA, Scheduling Staff ****	Scheduler, Conciliators, All other J's, Pro'tary NOVO staff	NOVO: although not a scheduling app, you can get some info indirectly by filtering records	√			√	JEIN, CIS, NOVO	
The content used for judicial education programs	J, JA w J consent, Law	J's of ct, NJI, presenters, host		√	√		√	Judicom	

Information gathered, produced or used for judicial purposes  (as discussed at our meeting on May 24 and , in this column, limited to that related directly to a judge)	Access	Others who gather, produce, use document/s listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
(ltd to J)	Clerk	staff, librarian							
Information regarding a particular judge's attendance at educational programs*****	J, JA, scheduling staff, Chief, ACJ,+EAs			√	√			CIS, JEIN	
Statistics showing a judge's individual activity or workload	J, CJ, ACJ	DoJ, CAs, Schedulers		√				NOVO,CIS	
Personal notes, research or working papers produced by or on behalf of a judge that have not been deposited on a <i>Case File</i>	J, JA + Law Clerk with J consent			√	I,C,F		√		
Judicial committee including communication, research material	J	Committees Chiefs, Ex Office	Some committee material further restricted to judicial-only members vs. all members	√	√		√	√ (e.g. ACTC materials in FileNet)	
Judicial benchbooks	J			√	√				
Search warrants, PSRs									

Information gathered, produced or used for judicial purposes  (as discussed at our meeting on May 24 and , in this column, limited to that related directly to a judge)	Access	Others who gather, produce, use document/s listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
Special recordings		NOVO users						NOVO	
Reports- medical, psych, financial									
Judicial Disciplinary									

\*Who else could create, read, update, distribute or Repackage (rebundle, extract metadata, add value, etc.) this type of information?

\*\* Court of Appeal has some differences specific to that court

\*\*\* More discussion needed on the to/from issue

\*\*\*\* Varies from court to court. Need to clarify.

\*\*\*\*\* Need to clarify or indicate the type of information, ie attendance only, where, when, etc

# ANNEXE B

Information gathered, produced or used for judicial purposes	Access	Others who gather, produce, use information listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I,J	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS 1 & 2, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
<b>Blank electronic forms, templates (some examples: Decision and Division of Assets Templates, Pre-trial Conference Report forms, stationary templates) *Note: the forms and templates are created by and used by judicial users and consist of boilerplate and no actual 'content' as would a completed form.</b>	Currently: all of NSGOV can read; should be judicial users even though info here is (currently) considered low to moderate security	Judges, JAs, Publication Manager, Comm. Director, JITSO		√	C,F,I			FileNet	Web server
<b>Court Policies (ACTC Policies, Electronic Devices in Courtrooms, Media Guidelines, etc.) *created by and for judicial users</b>	ACTC Members (judicial) ,Exec Office, Judges, Chiefs & ACJs, committees	JAs, DoJ, CIO	Once produced, this info is often distributed to many DoJ or CIO users	√	C,F,I			Outlook, FileNet	Web Server (courts.intra)
<b>Courthouse Telephone lists containing direct lines or cell numbers for judges (*Note: see blue sheet Contact Details. Would this be similar?)</b>				√	C,F,I				
<b>Emergency Contact Lists with Judges info (*Note: As above - see blue sheet Contact Details. Would this be similar?)</b>	List-creator only (e.g. Exec. Office; Court Admins?)	Judges, JAs, EA's, Sheriffs, Clerks by request only	Limited info divulged (e.g. office phone #) via phone	√	C,F,I				

Information gathered, produced or used for judicial purposes	Access	Others who gather, produce, use information listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I,J	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS 1 & 2, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
<b>Executive Office Black Binder (Judges' contact info includes private phone and addresses) (*Note: As above - see blue sheet Contact Details. Would this be similar?)</b>	Exec Office only	Judges, JAs, EA's, Clerks by request only	Limited info divulged (e.g. office phone #) via phone	√	I				
<b>Executive Office – all information produced by, except examples stated above (e.g. memos and materials created by various E.O. members)</b>	EO, Chiefs, Judges	Various Committees	Only as committee deliverables; CIO, DoJ when necessary	√	C,F,I			Outlook	Courts.intra
<b>Video Conferencing (mobile systems)</b>		DOJ	DOJ – for quality assurance & troubleshooting, logging of sessions is encouraged	√					CIO bridge (on occasion)
<b>Video Conferencing – desktop (Lync)</b>									
<b>Court Webcasting</b>									Archived videos on Web server
<b>Court Rules, Forms, Amendments, Practice Memos, Directions, Transcripts, Library Sheets</b> *The electronic versions which are archived in FileNet	Judges and JAs, Pub. Mgr	Prothonotary?, Law Clerks?		√	√			FileNet (primary repository)	
<b>Weekly Lists</b>	Created by Pub							Courts.intra website	

Information gathered, produced or used for judicial purposes	Access	Others who gather, produce, use information listed*	Access in relation to column 3	Where Stored					
				Paper	Drive C,F,I,J	Personal Device	Printer (hard drive, memory)	System /Application (FileNet, CIS 1 & 2, JEIN, Outlook, NOVO, etc.)	Network Hardware / Appliance
	Mgr. for Judges								
<b>Decisions (redacted, corrected...) Erratum</b> *The electronic versions which are archived in FileNet	Judges, JAs, Pub Mgr.	Prothonotary?, Law Clerks?						Filenet	