Canadian
Judicial Council

Conseil canadien
de la magistrature

Canadian Judicial Council

GUIDELINES FOR MIGRATION OF JUDICIAL INFORMATION TO A CLOUD SERVICE PROVIDER

Prepared by Martin Felsky, PhD, JD
Special Advisor to the CJC on Information Technology

September 2019

CONTENTS

BACKGROUND

The prospect of migration to the cloud raises several concerns for judges.[1] These guidelines were prepared at the request of the Technology sub-Committee of Council, to assist judges across Canada as they consider whether to move to the cloud with their respective administrations, and if so under what circumstances. The guidelines are divided into four major sections:

1. Prerequisites
2. Independence
3. Other Security and Privacy
4. Service Level and Functionality

In each section, there is an indication of whether the guideline is a "must have" or a "nice to have".

[1] PREREQUISITES

Activities that the judiciary must undertake prior to cloud migration. These are "must haves."

[A] THREAT AND RISK ANALYSIS

Before moving sensitive data to the cloud, a threat and risk analysis (TRA) should be performed. Entrusting judicial information to any computer system requires an understanding of the associated risks. A threat and risk assessment is the foundation for classifying information into appropriate levels of required protection. Security policies flow from the results of a threat and risk assessment.

The *Harmonized TRA Methodology (TRA-1)* was prepared by the Canadian Cyber Incident Response Centre (now part of the Canadian Centre for Cyber Security) and serves as a useful

[1] A fuller discussion is available in *"Judicial Information in the Cloud: The Case for Independence"*, prepared by Martin Felsky for the Canadian Judicial Council in August 21, 2018.

standardized model not only for conducting a TRA, but also for drafting a statement of work for TRA consulting services. See https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1.

There are other TRA templates available. Courts may choose to follow any model appropriate to their situation. For example, the Government of Saskatchewan developed a *Threat Risk Assessment Template* (2018) which is only available in English and can be found at: https://taskroom.sp.saskatchewan.ca/Documents/Threat-Risk-Assessment-Template.pdf

[B] PRIVACY IMPACT ASSESSMENT (PIA)

Before information is migrated to a new system, an assessment should be made to determine whether it contains personal information that may be subject to privacy and access laws, and how to deal with applicable protections, consents, access, retention and other requirements.

Typical steps involved in a PIA, according to the Office of the Privacy Commissioner of Canada (OPC) are as follows[2]:

- Identifying all of the personal information related to a program or service and then looking at how it will be used;
- Applying the OPC's four-part test for necessity and proportionality to highly intrusive initiatives or technologies (see OPC's *Expectations* document for more information at: https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_201103/);
- Applying the ten privacy principles;
- Mapping where personal data is sent after it is collected;
- Identifying privacy risks and the level of those risks; and
- Finding ways to eliminate or reduce privacy risks at an acceptable level.

Like TRAs, privacy impact assessments can be conducted in accordance with a template appropriate to the jurisdiction. For example, the Government of Nova Scotia's PIA template which is only available in English and can be found at: https://novascotia.ca/just/IAP/_docs/Appendix%20B%20PIA%20Template.pdf

[2] Office of the Privacy Commissioner of Canada,https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_33/.

The Government of Canada *Directive on Privacy Impact Assessment* can be found at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

[C] DEFINE JUDICIAL INFORMATION

Judicial information needs to be defined and differentiated from other information, e.g. court information or judges' personal information.

"Moving to the cloud" raises the basic question – moving what exactly? The most basic migration is usually to a hosted email system and document repository (for example Microsoft Outlook and OneDrive or SharePoint.) The judiciary must define the information that belongs exclusively to the judiciary, compared with, say, court records or court administration information.

[D] DEFINE JUDICIAL USERS

1. For the purposes of access and permissions, determine who is a "judicial user" and the appropriate permissions level required for their role.
2. Develop a process for user additions, deletions and permissions, and a policy for third party access (if any).
3. Draft and adopt security clearance requirements for anyone with access to physical servers

It is recommended that the definitions of judicial information and judicial users be standardized as much as possible for all courts. A consistent definition will make cloud migration and information management in the cloud simpler and less costly. The key reference here is the Canadian Judicial Council's discussion paper *Court Information Management Policy Framework to Accommodate the Digital Environment* (2013): http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf.

A summary of the key points included in the 69-page report relating to these definitions is available in Appendix 2A of the report (pp. 61-63). The report contains templates to assist courts in the definition process.

Two helpful documents from the Nova Scotia Courts Judicial Information System project are attached (Annexes A and B), as examples of the templates in action. Available in English only.

[E] CLASSIFY JUDICIAL INFORMATION

Judicial data needs to be classified in accordance with its sensitivity.

Not all "judicial information" – as defined – necessarily requires the same level of protection. The *Blueprint for the Security of Judicial Information* recommends that judicial information be classified according to its sensitivity, which would be an outcome of the threat and risk assessment. ..\Blueprint\Canadian Judicial Council Blueprint for the Security of Judicial Information - Fifth edition, 2018.pdf

[F] DATA RESIDENCY

Data residency (including OneDrive and SharePoint) must remain in Canada (at rest, and including backups). While in transit, data should reside in Canada, where feasible.

[G] RECORDS MANAGEMENT

1. The judiciary must decide how cloud data is disposed of when files are deleted or a user retires.
2. The judiciary must decide whether the cloud will act as data archive for the long term.
3. The judiciary must have a plan for the end of the hosting contract and the orderly transfer of data to another host.

[H] TRAINING

Notwithstanding the best security infrastructure and encryption available, most security breaches are the result of end-user behaviour. For this reason, thorough and regular information security training must be available to all users of any system containing judicial information.

[2] INDEPENDENCE

These are all must haves - or otherwise as described below.

1. Using the same cloud service provider would make it easier to migrate to a community cloud for judges in the future.
2. It may be preferable for judicial users to have their own tenancy rather than shared.
3. Judicial users should have their own email domain.
4. Contract terms available to judges.
5. Address potential conflicts between Microsoft and judicial policies.
6. Double-key end-to-end encryption (by default), with a second key controlled by the judiciary.
7. Login screen message cannot be customized - so government should add disclaimer for judicial users.
8. Cloud provider must follow specific policies re notification of a security or privacy breach. (see also Other Security and Privacy)
9. Judiciary can develop unique security policies to deal with personal devices that access sensitive content.

[3] OTHER SECURITY AND PRIVACY

These are all consistent with the requirements of the *Blueprint for the Security of Judicial Information* and should thus be considered "must haves."

1. Determine the limit to the level of sensitivity of information that provider is willing to host. (For example Shared Services cloud services are only for unclassified information)
2. Cloud provider must follow specific policies re notification of a security or privacy breach. (see also Independence)
3. Cloud provider should offer redundancy (including redundant network links) and quick time for fail-over to kick in (business continuity). (see also Service Level and Functionality)
4. End-user encryption with training.
5. Users see who attempted (and who succeeded) to access an encrypted document.
6. Users can restrict which recipients can read, edit, print or forward an email or document.
7. Measures to prevent unauthorized access.

8. Privileged access logs available to the judiciary.
9. 24/7 cyber security protections.
10. Restricted administrator access.
11. Audit of privileged administrator access to judicial users/data, with alerts.
12. Multi-factor authentication.
13. The host should perform penetration testing.
14. The cloud provider must back up data.
15. The host must have a disaster recovery plan.
16. The host must have network monitoring strategy and process to monitor network traffic. (see also Independence)
17. Compliance with the *Blueprint for the Security of Judicial Information* and international security standards.
18. Regular third party security audits.
19. Judiciary can develop unique security policies to deal with personal devices that access sensitive content. (see also Independence)

[4] SERVICE LEVEL AND FUNCTIONALITY

Whether these are must haves or nice to haves, they can be negotiated according to local preference.

1. Interoperability with court systems (may conflict to an extent with judicial independence).
2. There must be in place a Service Level Agreement which identifies the hosting provider's response time.
3. Host must provide adequate service desk hours.
4. 99.9% availability with no scheduled downtime.
5. Cloud provider should offer redundancy (including redundant network links) and quick time for fail-over to kick in (business continuity). (see also Other Security and Privacy)
6. The host must have a communications plan to notify users of planned and unplanned outages.

ANNEX 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 *Case File* 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	0, 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	0, 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 *Case File*		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 *Case File*	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

ANNEX 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
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.**	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
Court Policies (ACTC Policies, Electronic Devices in Courtrooms, Media Guidelines, etc.) ***created by and for judicial users**	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)
Courthouse Telephone lists containing direct lines or cell numbers for judges **(*Note: see blue sheet Contact Details. Would this be similar?)**				√	C,F,I				
Emergency Contact Lists with Judges info **(*Note: As above - see blue sheet Contact Details. Would this be similar?)**	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
Executive Office Black Binder (Judges' contact info includes private phone and addresses) **(*Note: As above - see blue sheet Contact Details. Would this be similar?)**	Exec Office only	Judges, JAs, EA's, Clerks by request only	Limited info divulged (e.g. office phone #) via phone	√	I				
Executive Office – all information produced by, except examples stated above (e.g. memos and materials created by various E.O. members)	EO, Chiefs, Judges	Various Committees	Only as committee deliverables; CIO, DoJ when necessary	√	C,F,I			Outlook	Courts.intra
Video Conferencing (mobile systems)		DOJ	DOJ – for quality assurance & troubleshooting, logging of sessions is encouraged	√					CIO bridge (on occasion)
Video Conferencing – desktop (Lync)									
Court Webcasting									Archived videos on Web server
Court Rules, Forms, Amendments, Practice Memos, Directions, Transcripts, Library Sheets ***The electronic versions which are archived in FileNet**	Judges and JAs, Pub. Mgr	Prothonotary?, Law Clerks?		√	√			FileNet (primary repository)	
Weekly Lists	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								
Decisions (redacted, corrected…) Erratum ***The electronic versions which are archived in FileNet**	Judges, JAs, Pub Mgr.	Prothonotary?, Law Clerks?						Filenet	