CJC
Canadian
Judicial Council

Blueprint for the Security of Court Information

Sixth edition, April 2021

Prepared by Martin Felsky, PhD, JD, for the Canadian Judicial Council

Table of Contents

INTRODUCTION TO THE SIXTH EDITION

Readers will note that this sixth edition of the Blueprint has a new title. Historically this document has applied to so-called "Judicial Information" as defined within its pages and subsequently as defined in the Canadian Judicial Council *Framework* publication.[1] Starting with this edition, the Council is confirming that the policies of the Blueprint apply - and in fact have always applied - to the broader category of Court Information as defined below. The Council's *Model Definition* report explains the reasons for this important change in terminology.

This revision also addresses another important development since the 2018 fifth edition. The worldwide Covid-19 pandemic severely limited the ability of courts throughout 2020 to operate effectively, and has driven many courts to adopt unfamiliar online procedures or accelerate the implementation of online services already in use. As a result, this Blueprint now covers security issues arising from the use of videoconferencing, e-filing and collaboration platforms.

The Blueprint has been drafted with the oversight of the Council's Technology Subcommittee, and in consultation with a national group of Judicial Information technology security officers, to whom the Council is grateful. Special thanks to Robert Gusnowski, Judicial Information Technology Security Officer, Alberta Courts, for his detailed suggestions, many of which have been incorporated.

BACKGROUND

The Canadian Judicial Council acted on several recommendations made in November 2001[2], which are based on the following fundamental principles:

- Judges and court administrators must make information technology security ("ITS") a priority in their courts.
- ITS is not merely a technical concern but involves planning, management, operations, and end-user practices.

[1] All key references are listed in Appendix 1 below.

[2] See Appendix 2. The full 2001 Report is confidential as it deals with potential vulnerabilities of court systems.

- All ITS measures taken by courts must safeguard judicial independence and other unique aspects of the relationship between Judicial Users and court IT administration, whether managed by government, a court services organization, or even the private sector.

- Responsibility for ITS policy with respect to the security of Judicial Information is a judicial function and, as such, rests with the judiciary.

- Management, operations and technical measures to safeguard Judicial Information in accordance with judicial policy are administrative functions, which in most courts are the responsibility of the provincial government.[3]

In 2013, the Council adopted sixteen foundational policies relating to Court Information governance, as set out in the *Framework*. The *Framework* also sets out policies for Access, Privacy, Security, Preservation, and Performance Management. The Blueprint was revised to conform to the applicable *Framework* policies.

The Blueprint is just one part of the Council's approach to the security of Judicial Information. For more information on the Council's related initiatives, please visit www.cjc-ccm.ca.

SCOPE AND DEFINITIONS

DEFINITIONS

The Blueprint uses the following key terms as redefined in the *Model Definition*. Readers are encouraged to refer to that report for more context and specific examples.

Term	Definition
Case File / *Dossier judiciaire*	A Case File contains the Information that relates directly to a single court proceeding or to a number of related court proceedings that have all been assigned the same case file number. It includes the Information that comprises the Court Record and any other Information that has been captured or placed in the Case File.

[3] This issue does not arise in federal courts such as the Supreme Court of Canada, however, the federal government considers the provision of internet services (through SCNet) to be a government function.

Court Information / *Information judiciaire*	Court Information is Information that is received, collected, stored, used or produced by a court in relation to its mission.
Court Operations Information	Information related to the supervision, management and direction of matters necessary for the operation of the Court or other matters assigned to the Executive by law or agreement (such as a Memorandum of Understanding). In Quebec, Case Management Tools (*Outils de gestion des causes*) and Court Monitoring Tools (*Outils de suivi des affaires judiciaires*) are included as subsets of the broad category of Court Records (*Documents d'activité des tribunaux*) and are probably best included under Court Operations Information.
Court Record / *Document judiciaire*	Information and other tangible items filed in proceedings and the information about those proceedings stored by the court. Refers to the "Official" recorded Information of a proceeding. It is the portion of the Case File that is made accessible to the public, subject to privacy constraints regarding, for example, disclosure of personal Information.
Information	Information includes recorded information in any medium or format, regardless of how it has been created. This includes information generated by human or other means.
Judicial Administration / *Administration judiciaire*	The supervision, management and direction of matters necessary for carrying out judicial functions, including: 1. the scheduling, preparation, assignment and adjudication of court events; 2. the education, performance, conduct and discipline of Judicial Users; 3. the governance of Court Information and technology, and 4. all other matters assigned to the judiciary by law or agreement (such as a Memorandum of Understanding).
Judicial Information / *Renseignements de la magistrature*[4]	Irrespective of who created it or how it was created, Judicial Information includes: 1. Personal Information of Judicial Officers; 2. Information related to the exercise of a judicial function ("Adjudicative Information"), and 3. Information related to Judicial Administration ("Administrative Information").

[4] While "*Information Judiciaire*" has been used for "Judicial Information" in the past, in French it means "Court Information." To avoid confusion, "Judicial Information" should be translated as "*Renseignements de la magistrature*."

Judicial Agent / *Agente ou agent judiciaire*	A Judicial Agent is a Judicial User who supports a Judicial Officer and may include court staff such as executive officers, lawyers, paralegals, law clerks, JITSOs, law students, articling students, judicial clerks, administrative assistants, as well as independent consultants working under retainer or contract.
Judicial Officer / Officière ou officier judiciaire	A Judicial Officer is a Judicial User acting in a judicial or quasi-judicial capacity, and includes judges, deputy judges, masters, justices of the peace, registrars, prothonotaries or anyone else authorized to act in an adjudicative role.
Judicial User / *Utilisateur ou utilisatrice judiciaire*	A Judicial User performs or supports judicial functions and may be authorized to access Judicial Information at various levels of permissions, depending on their role.

JUDICIARY

“The judiciary” is a term used throughout the Blueprint. For any particular policy, “the judiciary” may refer to the complement of judges on a particular court; the office of the Chief Justice of a court, a designated representative of the Chief Justice, or a committee of judges responsible for technology in a jurisdiction.

SCOPE

Though the statutory mandate of the Council is limited to federally-appointed judges, those judges often share technology platforms and resources with their provincially-appointed counterparts. For this reason, among others, collaboration on the development of security policies is encouraged. The Blueprint applies to any computer system that is used to access Court Information. This would include cloud services, home computers, removable media, data communication networks and mobile devices.

Information technology security is a complex field and the Blueprint is not intended to be comprehensive or technical in its scope. Furthermore, the Council’s focus is on the role of the judiciary in developing policies and standards, and not on the specifics of managing a technology department. In that respect, the Blueprint does not cover every aspect of security administration. Nor does the Blueprint discuss security relating to information that is not in digital form, security of telephone and fax communications, or the physical security of a courthouse and its occupants.

The Blueprint is designed to tailor and enhance existing policies and programs within governments and court administrations. To that extent, the Blueprint is based on and intended to co-exist with worldwide reputable information security standards, guidelines, controls and best practices, some of which are listed in the Key References section below.

SUMMARY OF KEY CHANGES TO THE SIXTH EDITION

1. Changed title to reflect the actual scope of judicial policy-making and to normalize English and French versions.
2. Added new policies relating to remote work, virtual hearings and collaboration platforms.
3. Provided new and updated definitions of key terms.
4. Re-ordered the policies for a more logical flow.
5. Updated references and hypertext links.
6. Removed Appendix 3 – Sample mobile device security policy.
7. Added and updated Glossary entries.

POLICIES

1. JUDICIAL INDEPENDENCE

Policy 1a: All information security measures taken by courts must safeguard judicial independence and other unique aspects of the relationship between Judicial Users and court administration, whether managed by government, a court services organization, or the private sector.

Policy 1b: Judicial Users must be provided with their own security domain, whether isolated by physical or logical separation, or a combination of both. Network architecture, configuration, access controls and operational support must at a minimum be compliant with the latest edition of the Blueprint.

Policy 1c: Regardless of who has custody or access, the judiciary always has ownership of Judicial Information.

Commentary:

Judicial independence is a fundamental constitutional principle. It applies, for the benefit of the public, to the judiciary in general as well as to individual judges. Independence includes freedom from any undue influence, but particularly independence from the executive branch of government, which is a frequent litigant before the courts. One of the key elements of judicial independence is administrative independence, to which the governance and application of information technology are tightly bound.[5] Because an independent judiciary engenders public trust in the system of justice, the *appearance* of independence must also be carefully safeguarded.

Cross references: NIST SP-800-171r2.

[5] "Our Constitution requires that judges at all levels enjoy security of tenure, financial security, administrative independence, and adjudicative autonomy." Hon. Ian Binnie, "Judicial Independence in Canada", http://www.venice.coe.int/WCCJ/Rio/Papers/CAN_Binnie_E.pdf, page 34 (checked 20201226).

Framework: All judiciary, court staff, and court communications will use a common Internet domain that is distinct from the government domain (Foundational Policy 8).

2. MONITORING

Policy 2**a**: Any monitoring of Judicial Users must be performed in accordance with the Canadian Judicial Council *Computer Monitoring Guidelines* (2002): "As an overriding principle, any computer monitoring of judges, and judicial staff who report directly to judges, must have a well-defined and justifiable purpose that does not encroach on deliberative secrecy, confidentiality, privacy rights or judicial independence."

Policy 2b: Analytical tools (including those incorporating artificial intelligence) may not be applied to Court Information, whether anonymized or not, without the advice and approval of the judiciary.

Commentary:

While content monitoring such as keystroke recording, review of web browsing history and automated keyword searching of emails would be a direct violation of judicial privacy including deliberative secrecy, any form of monitoring can potentially compromise judicial independence. For example, event logs can contain sensitive data and personally identifiable information. Judicial research may require access to websites that are routinely blocked for non-Judicial Users.

Cross references: NIST SP800-53r5, ISO 27001:2013 18.1.4. and ISO 29100.

Framework: Privacy Impact Assessments will be undertaken at the design stage of Court Information management systems that involve the potential collection, access, use, or dissemination of personal information (Privacy Policy 3).

3. POLICY

Policy 3a: Responsibility for Court Information policies, including information security, is a judicial function and, as such, rests with the judiciary. Management, operations and technical measures to safeguard Court Information in accordance with judicial policy are administrative functions, which in most courts are the responsibility of a government agency.

Policy 3b: Every court must plan and conduct an annual threat and risk assessment ("TRA") in collaboration with the judiciary. The level of detail required in a TRA, and its scope, may vary from one court to another depending on the circumstances.

Cross references: NIST SP800-53r5, 12-PL, 14-RA, ISO 27001:2013, A.5. See ISO/IEC 27005 for risk management guidance.

Framework: Information Management Policies will be published on the Court web site (Access Policy 7).

4. GOVERNANCE

Policy 4: The security of Court Information must be managed within a formal, documented security program authorized and adequately funded by the government body responsible for court administration. Court administration must describe in a written plan how the security requirements of the judiciary are to be met.

Commentary:

The security of Court Information cannot be left to *ad hoc*, informal and undocumented processes, nor can ultimate responsibility be delegated to junior level employees. Adequate budgets must be allocated to ensure the security and integrity of Court Information, in accordance with the threat and risk assessment.

Cross references: ISO 27001:2013, A.6.

5. JUDICIAL INFORMATION TECHNOLOGY SECURITY OFFICER

Policy 5: Every jurisdiction must ensure that a Judicial IT Security Officer (JITSO) who is accountable to the judiciary be appointed to oversee the management of Court Information technology security operations.

The primary role of the JITSO is to advise the judiciary in its negotiations and close co-operation with court administration and third-party providers on issues relating to information security. The key element is that the role must be functionally accountable only to the judiciary, to avoid any potential conflicts of interest. In some jurisdictions the JITSO may be part of an organization providing support to Judicial Users, and specific qualifications, roles and responsibilities of a JITSO team should be determined by the needs of each court.

6. AWARENESS AND TRAINING

Policy 6: Adequate privacy and security awareness training must be provided to all system users including Judicial Users, while more advanced role-related training must be provided to any user with access to Court Information.

Commentary:

End users without adequate training present a real threat to any organization. Security awareness, awareness training, and education are all necessary for the successful implementation of any information security program. The training program should include material on the independence of the judiciary and the special constitutional position of Judicial Users.

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

7. PHYSICAL SECURITY

Policy 7: All processing facilities or equipment used for Court Information must be located in a physically secure environment, with access limited to authorized individuals. Physical security must be designed to protect Court Information assets from natural disasters or human threats, consistent with the threat and risk assessment.

Commentary:

Physical security refers to the protection of building sites and equipment (and information and software contained therein) from break-ins, theft, vandalism, natural or unnatural disasters, and accidental damage. Managers must be concerned with data centre construction, room assignments, emergency action procedures, regulations that govern equipment placement and use, energy and water supplies, product handling—and relationships with staff, outside contractors, other courts, government departments, agencies and tribunals. This applies whether equipment in on premises or not, and includes physical security of assets used to access Court Information remotely.

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

8. INFORMATION SYSTEMS

Policy 8: The processes for acquisition, development and maintenance of Court Information systems must be designed and applied so as to safeguard its quality, integrity and long-term availability. Judicial Information requires additional protection over and above the security safeguards applied to Court Information more generally.

Commentary:

In addition to low-level hacking, random login attempts and social engineering, court administrators should be mindful of the risks associated with advanced persistent threats.

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

Framework: Foundational Policy 10, Security Policy 5.

9. COMMUNICATIONS AND OPERATIONS

Policy 9a: Court security programs must include documented and approved operational controls, procedures, practices, and well-defined responsibilities. Additional formal policies, procedures, and controls must be used to protect the exchange and publication of Court Information through any type of communication medium or technology.

Policy 9b: Courts are responsible for implementing controls to protect against malicious code, denial of service attacks and similar external threats.

Commentary:

The key elements of operational security as defined in ISO 27001:2013 are:

1. Documented operating procedures
2. Change management
3. Capacity management
4. Separation of development, testing and operational environments
5. Protection from malware
6. Backup
7. Logging and monitoring
8. Clock synchronization
9. Control of operational software
10. Installation of software on operational systems
11. Technical vulnerability management
12. Restrictions on software installations
13. Information systems audit controls

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

Framework: Courts must implement and maintain updated best practices for securing wireless local area networks (WLANs) and ensuring that Judicial Users are not compromising the security of Court Information when using WLANs. (“Where a public wireless Internet access point is installed within a court precinct it must not compromise Court Information” Security Policy 6.)

Court Information systems and technologies should be procured, designed and implemented in a manner that facilitates interoperability and data exchange between different systems, all without compromising systems independence, judicial independence and the Courts' role as custodian of Court Records (Foundational Policy 4).

10. INCIDENT MANAGEMENT AND REPORTING

Policy 10: Every court must have in place a protocol for reporting of security incidents relating to or involving Judicial Users and Judicial Information to ensure that the principles of judicial independence are respected. Information security incidents must be reported promptly and only through approved channels.

Commentary:

Anyone who has reason to believe that a security breach is threatened or has occurred must take steps to report the incident, report it promptly, and report it to the appropriate person or persons. An incident reporting process includes awareness and training for all staff with respect to security safeguards, the warning signs of a breach, and the appropriate mechanisms for reporting.

Among the various types of security breaches include public release of court records subject to publication ban, or prior to approved release by the court.

The *Monitoring Guidelines* provides: “Any monitoring should be administered by personnel who report directly and are answerable only to the court's chief justice.” This principle should apply equally to the reporting of incidents involving Judicial Users.

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

11. BUSINESS CONTINUITY

Policy 11: Courts must protect Court Information in the event of a catastrophe, pandemic or other system failure, and provide a high level of assurance that any disruption in service as a result of such event will be as brief as possible. Judicial Users must have access to data storage that is securely backed up at least daily. Effective provision must be made to facilitate back up of Court Information created or received (if stored locally), for example on mobile devices.

Commentary:

A business continuity plan must be prepared based on the TRA and should include a process for updating. All business continuity plans must be consistent with the Blueprint and include at a minimum the following elements:[6]

1. Governance
2. Business Impact Analysis
3. Plans, measures, and arrangements for business continuity
4. Readiness procedures, testing and training
5. Quality assurance techniques (exercises, regular maintenance and auditing)

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

[6] For more information, see Government of Canada, Business Continuity Planning, https://www.canada.ca/en/services/policing/emergencies/continuity.html, English (checked 20201226). French: Planification de la continuité des activités, https://www.canada.ca/fr/services/police/urgences/continuite.html (checked 20210104).

12. PERSONNEL SECURITY

Policy 12a: All courts must ensure that there are documented procedures for orientation and departure, as well as ongoing training for employees and contractors who have access to Court Information. There must be processes in place to ensure that employees and contractors have the appropriate level of security. The procedures should provide for discipline in the event of a breach of the policies regarding the security of Court Information. Procedures must exist to ensure the removal of access when an employee or contractor departs or transitions to a new role.

Policy 12b: Users with access to Court Information should be granted only the minimum permissions required to perform their duties, in accordance with the principle of "least privilege."

Policy 12c: Access to Court Information may not be granted to an individual unless they meet the requirements of this Policy and have been granted government security clearance at a level corresponding with their role.

Commentary:

Before access to Court Information is granted, a user must have at a minimum:

1. a need to know
2. passed a police background security check
3. passed other applicable security screening procedures
4. been made aware of the special nature of Court Information ("Staff Training Strategies should be embraced to improve awareness of the sensitivity of Judicial Information" Framework Security Policy 4.)
5. trained in all applicable security policies, procedures and practices
6. signed an agreement that documents their obligations respecting the security of Court Information

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

Framework: Oaths of confidentiality will be contained in engagement contracts for employees, consultants and contractors to prevent inappropriate disclosure of sensitive Court Information (Security Policy 2).

13. ACCESS CONTROL

Policy 13a: With respect to Court Information, all access control decisions are the responsibility of the judiciary. Users should be provided with the minimum level of access required for their role and consistent with their security clearance level. Administrator access should be on an extremely limited basis to non-Judicial users for administrative support only. This non-Judicial access should be granted only on request and then removed when its immediate purpose is accomplished.

Policy 13b: Court Information systems containing Judicial Information must be held in an appropriately protected environment, with enhanced monitoring, stringent access controls and encryption where possible. Courts must establish sufficient logging on all servers and network devices to screen for unauthorized access attempts and aberrant usage patterns. Any such activity on the part of Judicial Users is always subject to the *Monitoring Guidelines* and must be brought to the attention of the judiciary.

Commentary:

This policy does not assume that the judiciary has exclusive authority to determine roles and security clearance; court administration must also have authority to determine appropriate user levels of access, because court staff have may dual reporting responsibilities. Based on the general principles outlined in the *Framework*, however, court administration cannot provide a user with greater access than that agreed to by the judiciary.

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

Framework: Bulk Access to a portion of or the entire Court Record shall be governed by written agreement with the court addressing key issues and risks (Access Policy 5).

Judicial Information must be protected from unauthorised access in accordance with the CJC's Blueprint for the Security of Court Information (Security Policy 1).

Audit logs must be closely monitored to clearly identify which users have access to Court Information at any point in time (Security Policy 3).

14. REMOTE WORK AND EXTERNAL SYSTEM ACCESS

Policy 14a: Courts must establish and document baselines for usage restrictions, system configurations, connection requirements, and implementation guidance for each type of remote access permitted.

Policy 14b: In consultation with the judiciary, Courts must establish specific terms and conditions for the use of external systems consistent with the Court's security policies and procedures and specify the highest security category of information that can be processed, stored or transmitted on external systems. Remote Judicial Users should be provided with adequate resources to meet the Court's security requirements.

Commentary:

Remote work is now a broader concept than remote access. Safe remote access is not just a matter for IT – but also important for individual working from home or elsewhere, especially on a regular basis. In addition, users – whether in the courthouse or elsewhere – are using external platforms and systems more often (in other words, software services that are not managed by court administration). Best practices should be developed and form part of a mandatory training program, which should include subjects such as physical security.

Cross references: Remote Access: NIST AC-17, Use of External Systems: NIST AC-20, Security Tips for Organizations with Remote Workers (ITSAP.10.016),[7] National Security Agency, Selecting and Safely Using Collaboration Services for Telework – UPDATE.[8]

[7] Canadian Centre for Cyber Security, https://cyber.gc.ca/en/guidance/telework-security-issues-itsap10016 (checked 20210108).

[8] https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/Collaboration_Services_UOO13459820_Full.PDF (checked 20200108).

15. MOBILE DEVICE MANAGEMENT

Policy 15: Courts must implement a Blueprint-compliant policy for mobile devices and implement security tools and protocols that allow for the wiping of data from lost or stolen devices.

Commentary:

Whether issued by court administration, used as part of an official “bring your own device” policy, or used outside of the court’s security program entirely, mobile devices are challenging traditional approaches to information security.

Mobile devices, whether provided by the court -- or, as is the dominant trend -- purchased by users themselves, invite many security risks.

1. Mobile devices can be configured to conveniently access networked information resources from anywhere. But unlike desktops or laptops, which are procured, issued, configured and maintained by court administration, mobile devices are typically not designed, nor built or configured with the same security capabilities in mind.
2. Mobile devices are computers that can generate, manipulate and store data. However, depending on configuration, password protection on these devices can be weak, encryption options may be limited or non-existent, and the devices can be easily misplaced or stolen, giving rise to serious security and privacy breaches.
3. The popularity of free and inexpensive apps has been largely responsible for the rise in popularity of mobile devices. Taking advantage of these apps is hugely convenient, but fraught with risk, as data created by the user and data about the user are transmitted - often surreptitiously -- to the third parties who make the software.
4. Mobile devices are always connected to the Internet, and with built-in GPS capabilities, track the location and activities of users in real time. If compromised, the built-in cameras and microphones can also be used to record and transmit events and conversations without the knowledge of the user.

16. CLASSIFICATION OF COURT INFORMATION

Policy 16a: Courts should adopt a classification scheme so that sensitive Court Information may be designated for special protection. Classification schemes as adopted should be consistent across all courts to ensure a common understanding of asset sensitivity and protection requirements.

Policy 16b: Classified information may be made available to a person only when the originator establishes that the person has a valid "need to know," appropriate personnel security controls are in place, and the access is necessary to the accomplishment of official court duties.

Commentary:

The author of a document should be responsible for assigning the appropriate classification to information that he or she has created. Documents cleared for public access may be declassified (or as the case may be, unclassified from the start). Everyone who works with the Court has a duty to respect the confidentiality and integrity of any court information and data that they access, and is personally accountable for safeguarding assets in accordance with this policy.

The following three-level classification scheme provides one model that could be used in a court. Other approaches can be adopted to meet local needs, though consistency from one jurisdiction to another would be preferable. Court administrators may require enhanced controls to manage security and privacy risks to aggregated data or to manage integrity and availability concerns.

> **Court-Official** – Most Court Information is by default classified as "Official" and is therefore subject to the protections outlined in the Blueprint. This includes routine administrative operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. There is no requirement to explicitly mark routine "Court-Official" information.
>
> **Court-Restricted** – This classification is used for sensitive Court Information, for example: documents containing personal information that may relate to judges, matters or parties; draft judgments, e-mails relating to judicial opinion and case

law, and memoranda about issues affecting the judiciary. Restricted Court Information would be subject to more stringent treatment than Court-Official, including special markings, encryption, and storage on designated devices. All such information should be clearly and conspicuously marked "COURT-RESTRICTED."

Court-Secret – This classification is used for the most sensitive Court Information, including, for example, government intelligence, sealed case files, and police reports requiring the highest levels of protection from the most serious threats. Original source markings should also be left in place. All such information should be clearly and conspicuously marked "COURT-SECRET."

The originator is responsible for classifying and marking the information, and may also decide to change classifications or declassify as needed.

Documents may be upgraded, downgraded or declassified as necessary, with the proper authority. For example, when a draft judgment (marked "COURT-RESTRICTED") is finalized and ready for public release in accordance with the judge's instructions, it should be marked "COURT-DECLASSIFIED" and the date of declassification shown. Over time, the classifications of a document or other asset may be modified depending on an expired time frame or a routine re-evaluation.

When working with information assets, the following points must be considered[9]:

1. Applying too high a classification can inhibit sharing and lead to unnecessary and expensive protective controls; applying too low a classification may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.

2. When working with documents, classification labels must be in CAPITALS at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed with fewer restrictions.

3. Sensitive material shared internally must also be clearly marked.

[9] Derived from UK Cabinet Office, Government Security Classifications, May 2018 version 1.1.

4. It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable systems should compel users to select a classification before sending, e.g., via a drop-down menu.

5. A file, or group of sensitive documents or assets, must be labelled with the highest classification of information contained within it. For example, a paper file or an e-mail thread containing COURT-OFFICIAL and COURT-SECRET material must be covered by the higher marking (i.e., COURT-SECRET).

6. E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail thread before they add to it and forward it on.

7. In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitized digest or pre-agreed form of words at a lower classification in anticipation of such a requirement.

Cross references: Asset Management ISO 27001:2013, A.8, UK Cabinet Office, Government Security Classifications, May 2018 version 1.1.

17. ENCRYPTION AND SIGNATURES

Policy 17a: The judiciary must be involved in the development of encryption policy and implementation, as they relate to confidentiality, integrity, non-repudiation and authentication of Court Information. Encryption policy and procedures should be consistent with the classification scheme for Court Information. Key management, including policies and procedures, must be in the hands of the judiciary.

Policy 17b: To ensure complete independence, it is recommended that the certificate authority for Judicial Users be a trusted third party independent of government.

Policy 17c: The decision to encrypt data should be based on documented court security risk management decisions and the application of the Court Information classification scheme.

Policy 17d: Courts should provision authorized Judicial Users with secure digital or electronic signatures to facilitate secure workflows in a virtual court setting.

Commentary:

The objective of this policy is to make encryption tools readily available to Judicial Users, manage the encryption process securely, ensure that judicial independence is preserved, and protect sensitive information from unauthorized access. The application of a digital signature is an important tool for protecting the integrity and reliability of those court records that require a signature where courts are operating in a paperless environment.

Cross references: ISO 27001:2013A.10. ISO 27017:2015, s. 10, ISO 27002, 10.1, Secure Electronic Signature Regulations, SOR/2005-30, made under the Canada Evidence Act and PIPEDA (checked 2021-01-09).

18. CLOUD MIGRATION

Policy 18a: Court Information may not be migrated to the cloud without the consent of the judiciary and compliance with the mandatory prerequisites outlined in the *Cloud Guidelines*. As such, the judiciary must be included in negotiations for proposed cloud services including governance, operations, access controls, data location, and other security considerations.

Policy 18b: The security, privacy and integrity of Court Information must be expressly addressed in any service provider agreement. Third party compliance with the Blueprint must be monitored and audited on a regular basis.

Commentary:

Cloud computing allows users in different organizations to share hardware, network services and software from the same provider, but with each organization independently managing its own user access and information independently. This contrasts with traditional architectures in which each organization builds its own data centre and provisions its own networking equipment, hardware and software. The advantage of cloud computing is that by consolidating investment in physical space, management, hardware, software, communications, electrical power, backups and security, cloud service users only access and pay for the computing resources that they need, leaving the administration of the technology to their provider.

Consolidation from the government's perspective leads to greater control over technology spending and technology management. From the perspective of the judiciary, however, consolidation of network, computing and support services means a diminishment of control and greater uncertainty as to the safeguarding of Court Information. For this reason, the judiciary in each affected jurisdiction has canvassed for greater transparency and a stronger voice in the planning and implementation processes.

In general, if the executive branch is going to be provisioning information services for the judiciary, either directly or in partnership with commercial third parties, the judiciary must play an active role in specifying how it wants Court Information to be managed.

The following prerequisites for moving Judicial Information to the Cloud were considered mandatory by the Canadian Judicial Council in the *Cloud Guidelines*:

1. Threat and Risk Assessment
2. Privacy Impact Assessment
3. Definition of Judicial Information (now Court Information)
4. Definition of Judicial Users
5. Classification of Judicial Information (now Court Information)
6. Data residency in Canada - “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.”
7. Records Management
8. Training

Other requirements are set out in that document and should be consulted prior to and after migration.

Cross references: NIST SP800-53r5, 18-SA, ISO 27001:2013, A.15, Cloud Security Alliance Security Guidance Version 4, (checked 2020-12126). See also Communications Security Establishment, ITSB-105 Security Considerations for the Contracting of Public Cloud Computing Services – December 2014 (checked 2020-12-26).

CJC: Guidelines for Migration of Judicial Information to a Cloud Service Provider (2019). Checked 2021-02-09.

19. DATA LOCATION

Policy 19: Classified Court Information must be stored in a computing facility located within the geographic boundaries of Canada. Classified Court Information may not be put at risk of access by any foreign law enforcement authorities without a threat and risk assessment, privacy impact assessment, and prior approval by the judiciary.[10]

Commentary:

Classified Court Information (as described in Policy 16 and commentary) should at all times reside in Canada. Judicial Users must be notified and give prior consent if any Judicial Data is proposed to be stored, processed or transmitted outside Canadian jurisdictions or by hosts in Canada that are subject to intrusive foreign law. Court information that is intended for public access (that is, either unclassified or declassified information) is not subject to any security-related location restrictions.

Cross references: Treasury Board, Data Sovereignty and Public Cloud (Checked 2021-01-12).
Security Assessment and Authorization. NIST SP800-53r5, 15-CA (data location).

[10] As a prime example, the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) is a United States federal law enacted in 2018 by the passing of the Consolidated Appropriations Act, 2018, PL 115-141, section 105 Executive agreements on access to data by foreign governments. Primarily the CLOUD Act amends the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil. Wikipedia at https://en.wikipedia.org/wiki/CLOUD_Act. (Checked 20201226.)

20. VIRTUAL PROCEEDINGS – VIDEOCONFERENCING AND STREAMING

Policy 20a: Videoconferencing platforms selected for court proceedings must be secure enough to comply with the Blueprint. Any videoconferencing platform used for court proceedings must be carefully configured and tested in advance to ensure that proceedings are not disrupted. End users (including members of the public) should be advised as to the applicable protocol for video hearings as established by the presiding judge.

Policy 20b: Internet bandwidth provided to Judicial Users in a courthouse must be provisioned sufficiently for robust video and audio performance.

Policy 20c: To the extent that videoconferencing multimedia proceedings, including associated text-based content, may need to be recorded, sufficient secure data storage must be provisioned, subject to the Blueprint and in accordance with the classification of the information.

Policy 20d: Video proceedings that have been declassified by the presiding judge or judges may be posted on public video-sharing platforms such as YouTube or Vimeo, as long as appropriate settings, watermarks and notations are posted to reflect the court’s public access and usage policies.

Commentary:

The Covid-19 pandemic has accelerated the progress of courts from in-person to virtual proceedings, and from paper exhibits to electronic. Courts have been quick to adopt videoconferencing, either by extending their existing internal systems (such as Microsoft Teams, or Webex) to external users, or by licensing purpose-built commercial platforms such as Zoom.

Judicial Users operating within courts and remotely should be provisioned as much as possible with sufficient continuous bandwidth so as to support interruption- and interference-free video and audio connections.

Videoconferencing providers have published various guidelines and security best practices for their respective platforms to ensure against so-called “Zoom-bombing” and other disturbances. These should be followed carefully.

Some courts have adopted scripts for presiding judges that can be read to all participants at the beginning of a virtual hearing to orient users to an unfamiliar process. It is recommended that such a script or checklist include references to security issues such as privacy, confidentiality, prohibitions (if any) on recording and streaming proceedings as well as local equipment configurations if applicable

Cross-references: NSA, Selecting and Safely Using Collaboration Services for Telework – UPDATE (Nov 2020), Zoom recommendations (Checked 2021-01-12), Microsoft Teams security documentation (Checked 2021-01-12); Cisco Webex Meetings Security (Checked 2021-01-12).

21. VIRTUAL PROCEEDINGS – COLLABORATION (FILE SHARING)

Policy 21a: When procuring, configuring, and implementing collaboration tools such as file and exhibit sharing for virtual proceedings, courts must ensure that sufficient storage space is provisioned, and that appropriate security controls are in place for data uploads, data sharing and data storage. These may include encryption for classified information as well as an audit trail of uploads, file access, modification and deletion.

Policy 21b: Courts must ensure that end users are effectively authenticated to avoid unauthorized access.

Commentary:

Despite the attractive convenience, low (or no) cost of public file-sharing platforms such as Dropbox, Box.com and many others, Courts intending to share classified information for virtual proceedings should avoid consumer-oriented platforms unless their security is thoroughly vetted. Consideration should be given to the concept of a Canadian “Community cloud for judges” – in which the judiciary would have their own independent tenancy, specifically for purposes such as virtual collaboration.

Cross-references: Canadian Judicial Council, Guidelines for Migration of Judicial Information to a Cloud Service Provider, 2019. Checked 2020-02-09.

22. SOCIAL MEDIA

Policy 22: The judiciary is responsible for establishing security policies, codes of conduct and training programs for the use of social media by Judicial Users.

Commentary:

Social networks and media raise many questions for courts and judiciary, not least are those related to security and privacy. Among these are "insufficient authentication controls, cross site scripting, cross site request forgery, phishing, information leakage, injection flaws, information integrity and insufficient anti-automation."[11] Policies and training should address all known risks.

23. COMPLIANCE

Policy 23a: All Court Information policies, procedures and practices must comply with applicable laws, regulations and valid contractual requirements. Access to and use of compliance audit tools must be limited to a small number of authorized individuals only. Where audits are performed on Court Information and Judicial Users, these must be done in compliance with the Monitoring Guidelines.

Policy 23b: In circumstances where Court Information may need to be searched or otherwise accessed in response to a legal request, prior approval from the judiciary is required. The judiciary shall determine who is granted access, and what Court Information may be exempt from the search, review and disclosure processes.

Commentary:

It is important that any individual responsible for compliance auditing – whether they work on behalf of the courts, a courts administration service, a government ministry or a commercial third party – be authorized by the judiciary and informed of the method and scope of work in advance.

[11] Cited by Wu He, (2012),"A review of social media security risks and mitigation techniques", Journal of Systems and Information Technology, Vol. 14 Issue 2, pp. 171 – 180. https://www.researchgate.net/publication/263528558_A_review_of_social_media_security_risks_and_mitigation_techniques (checked 20201226).

Individuals performing such work should be advised to comply with the Monitoring Guidelines. Such terms and conditions should form a part of any MOU or third-party hosting arrangement.

Whether Court Information in any particular circumstance is exempt from litigation disclosure and information access (or freedom of information) requests or not, the process of searching, reviewing and ultimately producing Court Information must only be performed by or with the consent and under the direct oversight of the judiciary.

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

Framework: Privacy Impact Assessments will be undertaken at the design stage of Court Information management systems that involve the potential collection, access, use, or dissemination of personal information (Privacy Policy 3).

Access to and use of compliance audit tools must be limited to a small number of authorized individuals only. Audit logs will be closely monitored to clearly identify which users have access to Court Information at any point in time (Security Policy 3).

APPENDIX 1: KEY REFERENCES

The *Framework* provides a principled structure for determining a wide range of Court Information policies, of which information security is just one. Part of the mandate for updating the Blueprint, then, includes ensuring its consistency with the values, principles, policies and definitions enunciated in the *Framework*, to which the reader of the Blueprint should refer.

Cross references referred to in each Policy section are to the following documents unless otherwise indicated:

CANADIAN JUDICIAL COUNCIL PUBLICATIONS

- *Court Information Management: Policy Framework to Accommodate the Digital Environment*. Jo Sherman, 2013. ("Framework")
- *Guidelines for Migration of Judicial Information to a Cloud Service Provider*, Martin Felsky, 2019 (Checked 2021-01-12). ("Cloud Guidelines")
- *Lignes directrices Sur la migration De l'information judiciaire Vers un fournisseur de Services d'informatique en nuage*, Martin Felsky, 2019 (Checked 2021-01-12).
- *Model Definition of Judicial Information*, Martin Felsky, 2020 (Checked 2021-01-12). ("Model Definition")
- *Définition modèle des renseignements de la magistrature*, Martin Felsky, 2020 (Checked 2021-01-12).
- Computer Monitoring Guidelines, 2002 (Checked 2021-01-12). ("Monitoring Guidelines")

INTERNATIONAL STANDARDS AND BEST PRACTICES

- *Information Security Management*, ISO/IEC 27001 (2013) This standard was last reviewed and confirmed in 2019. (Checked 2021-01-12). The 2017 version is very similar and may be used as reference in place of the 2013 designated title.

- *Information Technology - Security Techniques - Code of practice for information security controls*, ISO/IEC 27002 (2013) (Checked 2021-01-12).

- *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publications SP800-53r5 – updated to September 2020 version, including updates as of 2020-12-10 (Checked 2021-01-12)

- *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* NIST Special Publications SP800-171 Rev 2 (published February 2020) (Checked 2021-01-12)

- UK Cabinet Office, *Government Security Classifications*, May 2018 version 1.1 (Checked 2021-01-12)

SELECT STANDARDS FROM CANADIAN JURISDICTIONS

- *British Columbia Information Security Policy* V4.0 (pdf), last revision 2018-09-21 (Checked 2021-01-12)
- *General security requirements for the protection of the integrity, confidentiality and availability of Government of Ontario networks and computer systems* (Checked 2021-01-12)
- Canadian Centre for Cyber Security (Checked 2021-01-12)

APPENDIX 2: RECOMMENDATIONS OF JTAC AS APPROVED BY COUNCIL, NOVEMBER 30, 2001

1. That the Canadian Judicial Council consider conducting a seminar at its next mid-year meeting to review urgent security issues identified in [the report on court computer security of the Judges Technology Advisory Committee].

2. That the Chair of the Canadian Judicial Council circulate the report to the Canadian Council of Chief Judges and Chief Justices.

3. That the Chair of the Canadian Judicial Council circulate the report to all Deputy Attorneys General with a request for their co-operation in implementing the recommendations.

4. That the Canadian Judicial Council request that the National Judicial Institute and the Office of the Commissioner for Federal Judicial Affairs coordinate the delivery of training [about computer security issues, including concerns about judicial independence and the integrity of Judicial Information] for federal and provincial judges, together with information technology staff.

5. That the Canadian Judicial Council ask all provincially and federally appointed chief justices/judges to:

   (a) Establish security of the court's information system as a priority;

   (b) Ensure that policy development takes place at an early stage before the conversion to an electronic environment;

   (c) Identify and secure the necessary financial, staff and other resources that are critical to implementation of appropriate security measures;

   (d) Ensure that a technology staff member who is accountable to the chief justice/chief judge be appointed to manage the court's security operations.

6. To achieve uniformity, that the Canadian Judicial Council take a leadership role by authorizing the Judges Technology Advisory Committee to develop a blueprint that addresses recommended security procedures for all Canadian courts, and ensure that resources are made available to the Committee for that purpose.

APPENDIX 3: GLOSSARY OF TECHNICAL TERMS AND ACRONYMS

Term	Meaning
APT – Advanced Persistent Threats	High-level unauthorized network intrusions that persist undetected for long periods of time.[12]
Analytics	The application of advanced software tools used to discover and extract meaningful information from volumes of data.
Anonymization	The process of removing personal identifiers from collections of data.
Apps	Software applications that are downloaded for use on mobile devices.
BYOD	Stands for "Bring your own device" a policy that allows users to access business networks using mobile devices belonging to them personally.
Classification	The designation and marking of records with various levels of sensitivity.
Cloud	The term used to refer to data centres managed by third parties (a Cloud Service Provider) to host an organization's data offsite.
CSP	Cloud service provider. The two largest CSPs with data centres located in Canada are Microsoft Azure and Amazon Web Services.
Digital signature	A digital signature is an encoded message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission. Cf e-signature.
Encryption	A process that translates human-readable text into unreadable code for the purpose of securing information from unauthorized access.
Electronic signature (e-signature). Cf. Digital signature.	An e-signature is a form of signature applied to an electronic document, sometimes distinguished from a digital signature, which is an encoded form of authentication.
Firewall	A hardware or software product programmed to filter unwanted intrusions from one computer or network into another.
IDS	Intrusion Detection System – a system that monitors attempts to gain access to a network. Intrusion is defined as an attempt to compromise the security of a computer or network. Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of intrusions.

[12] According to a Bell Canada study (the "Dark Space Project", 2013, the widespread presence of APTs was uncovered in Canadian government and critical infrastructure: http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf (checked 20200104).

Term	Meaning
Integrity	Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
ISP	Information Service Provider – organization that provides access to the Internet.
LAN	Local Area Network – a system connecting users to shared computing resources within a building.
Least privilege	Least Privilege is the principle of allowing users or applications the least number of permissions necessary to perform their intended function.
Malicious code	Harmful programs and snippets of applications that are designed to delete data, prevent access, or otherwise interfere with the proper functioning of a computer system - the generic term for computer viruses, worms, spyware, Trojan horse, malware, denial of service attacks etc.
Malware	A generic term for a number of different types of malicious code. Cf Malicious code.
MOU	Memorandum of understanding – an agreement between the judiciary and a government minister setting out their respective roles and responsibilities for court and judicial administration.
Phishing	The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically, the e-mail and the web site look like they are part of a bank with which the user is doing business.
Physical security	Physical security refers to the protection of building sites and equipment (and information and software contained therein) from break-ins, theft, vandalism, natural or unnatural disasters, and accidental damage.
Public Key Infrastructure (PKI)	A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
Ransomware	A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.
Role based access control	Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.
Shared services	Shared services is a model of provisioning computing and networking services to an enterprise (such as a government) through a single centralized resource as opposed to having separate IT infrastructures in each component of the enterprise.
Service level agreement (SLA)	An SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties, usually defining a minimum “level of service" for availability, serviceability, performance, operation, or other attributes of the service.

Term	Meaning
Social engineering	Non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.
Spoof	Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
Threat and Risk Assessment (TRA)	Threat and Risk Assessment - the process by which risks are identified and the impact of those risks determined. A threat is a potential violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Virtualization	The configuration of a single central processing unit (CPU) to run more than one operating system at the same time, allowing an enterprise to better manage updates and rapid changes to the operating system and applications.
Virus	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
Virtual Private Network (VPN)	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network
Wired Equivalent Privacy (WEP)	A security protocol for wireless local area networks defined in the standard IEEE 802.11b.
Wireless LAN (also Wi Fi)	A local area network using radio frequency rather than wires to connect.
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.