Blueprint for the Security of Judicial Information

Fifth edition, 2018

Prepared by Martin Felsky, PhD, JD, for the Executive Committee of the Canadian Judicial Council, August 31, 2018

TABLE OF CONTENTS

INTRODUCTION TO THE FIFTH EDITION

To address concerns about security in the early 2000s, the first Blueprint had three purposes:

1. Provide guidelines to improve the security, accessibility and integrity of Judicial Information.
2. Define the respective roles and responsibilities of judges and administrators when it comes to information technology security and enhance the relationship between the two groups.
3. Provide judges across Canada with a model for the development of effective information technology security policies that take the principles of judicial independence into account.

Today it is fair to say that while these three objectives are still as valid as ever, their relative priority has shifted.

Comprehensive security program standards and prescriptive security controls are readily available and widely used by governments and private sector organizations. Interest in cybersecurity, which focuses on threats from the Internet, has seen explosive growth. Today's challenge is in understanding, interpreting and applying the principles of judicial independence in a cost-effective way, especially as governments move to centralize technology platforms for the entire public service.

The distinctive roles of judges and administrators are still imprecise, though the landscape has changed in twenty years. In almost every jurisdiction today there is a Judicial Information Technology Security Officer ("JITSO"), in line with the Council's recommendation.[1]

The policy gaps that have existed for some time are becoming more acute as governments are centralizing technology platforms and planning their migrations to the cloud. Beyond the narrow focus of security, matters of broader governance for Judicial Information must move more quickly into the spotlight.

ACKNOWLEDGMENT

The Blueprint has been drafted in consultation with a national group of judicial information technology security officers, to whom the Council is grateful.

[1] As of this writing, JITSOs have been appointed in eight of the ten provinces, two of the three territories, the Federal Courts and the Supreme Court of Canada.

INTRODUCTION TO THE FOURTH EDITION, 2013

The Blueprint is intended to serve several purposes. Its primary objective is to provide guidelines to improve the security, accessibility and integrity of Judicial Information. Another purpose is to clearly define the respective roles and responsibilities of judges and administrators when it comes to information technology security, and to enhance the relationship between the two groups. Finally, the Blueprint is designed to provide judges across Canada with a model for the development of effective information technology security policies that take principles of judicial independence into account.

The Canadian Judicial Council ("the Council") is pleased that since the publication of the first edition of the Blueprint in 2004, many courts have adopted security policies derived from and consistent with its terms.[2] Early concerns that the level of security provided for Judicial Information across Canada is uneven and inconsistent from jurisdiction to jurisdiction have to a great extent been addressed. The Council believes that courts and judges should continue to standardize the approach taken to the security of Judicial Information as much as possible among all courts. Best practices should be determined, implemented and kept up to date in all cases.

The Council is still concerned that in some courts, judges may not be involved in a policy-making role. The Council would like to ensure that wherever possible, judges have a role in policy-making and that all security measures undertaken in the courts are consistent with the fundamental principles of judicial independence.

Information security for judges presents practical challenges because of Canada's unique constitutional situation. For example, in most courts, non-judicial administrators provide all information technology ("IT") services to judges. Not only is there often no clear dividing line between judges and non-judicial administrators or users, but there is also rarely any reporting relationship between them. This can make it as difficult for administrators to gain judicial co-operation with IT policy as it does for judges to direct the work of technical support staff.

The Council suggests that IT administrators, support and help desk staff working with Judicial Users be made aware of the nature of the judicial role and function within the administration of justice. IT administrators, support and help desk staff must differentiate between Judicial Users and non-judicial users to preserve the independence of the judiciary.

The Canadian Judicial Council acted on several recommendations made in November 2001[3], which are based on the following fundamental principles:

---

[2] As of this writing, courts in British Columbia, Alberta, Saskatchewan, Ontario, Quebec, New Brunswick, Nova Scotia and PEI have appointed individuals or teams to fulfill the role described in the Blueprint as the "Judicial Information Technology Security Officer". The Supreme Court of Canada and federal Courts Administration Services have also designated individuals in that role.

[3] See Appendix 1. The full 2001 Report is confidential as it deals with potential vulnerabilities of court systems.

- 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.
- 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.[4]

More recently, 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 has been rewritten 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.gc.ca.

SCOPE AND DEFINITIONS

DEFINITIONS

JUDICIAL USER

The Framework[5] defines "Judicial Officer" as "a person 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". Throughout the Blueprint, the term "Judicial User" includes Judicial Officers and the broader range of individuals who have access to Judicial Information.

[4] 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.

[5] Jo Sherman, Court Information Management Policy Framework to Accommodate the Digital Environment, Canadian Judicial Council 2013 at http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf.

JUDICIAL INFORMATION

There is no generally accepted definition of "judicial information." In the Framework, however, the definition of "Judicial Information" is discussed. The Framework notes that the concept of "judicial information" may also overlap with defined terms such as "Case Files" and "Court Record", which are elements of "Court Information." The Council proposes that the Framework Report definitions be used as a model that can provide some consistency from one jurisdiction to another. These definitions are now used in the Blueprint:

Judicial Information is information stored, received, produced or used by or for a Judicial Officer. It also includes information stored, received, produced or used by staff or contractors working directly for or on behalf of judges such as executive officers, law clerks, law students, judicial clerks or assistants. [6]

There are three main types of Judicial Information:

Individual Judicial Information includes work product, research material and professional development information of Staff Lawyers, Law Clerks and Judicial Officers. This category would also include **Judicial Office Information** which includes judicial staff HR matters, judicial assignment information, statistics and court policies. Matters relating to judicial committee work could also fall under this definition.

General Judicial Information includes information used by Chief Justices, committee materials, statistics, research material, and court-wide professional development information.

Personal Judicial Information includes information produced by, on behalf of, or relating to a Judicial Officer that does not directly relate to the function or role of the Judicial Officer and is not associated with a Case.[7]

Examples of Judicial Information would include[8]:

- information relating to private or personal affairs and social interactions of a judge
- work relating to a Case File that is highly sensitive in nature (e.g. draft judgments)
- audit logs containing summaries of computer system activities undertaken by a judge
- history of web sites visited by a judge
- judicial email correspondence that does not directly relate to a Case File

[6] For the purposes of the Blueprint we would also propose to add "staff lawyers" to this grouping.

[7] Framework: "In each jurisdiction, it will be necessary to provide precise guidance to technologists in relation to Judicial Internet browsing history logs, email repositories, contact lists, calendars, text messages and voice mail when considering candidate information for [Personal Judicial Information]."

[8] Examples taken from Framework, page 33.

- sms (text) and voice mail messages
- diary and calendar events other than docket events that directly relate to a Case File
- contact details including address book information held on mobile phones or in desktop software applications or other electronic repositories
- 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
- information regarding the scheduling of judges within a court calendar
- the content used for judicial education programs
- information regarding a particular judge's attendance at educational programs
- statistics showing a judge's individual activity or workload
- personal notes, research or working papers produced by or on behalf of a judge that have not been deposited on a Case File
- judicial committee or board work including communication and research materials
- judicial benchbooks

It must be borne in mind that Judicial Information must be protected not only on active servers, mobile devices and storage media but in archival, imaged and backup systems as well.

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 for Judicial 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 government. To that extent, the Blueprint is intended to co-exist with worldwide 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 FIFTH EDITION

1. A general reorganization and update to address new technology and new priorities.
2. Expanded commentary sections.
3. Cross-referenced policies to controls in ISO 27001/2:2013 and NIST SP800-53r5 where appropriate.
4. Addresses comments and questions from stakeholders.
5. A newly drafted Acceptable Use Model Policy (Appendix 4).
6. Replaces the model SLA terms and conditions with a more useful reference.

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 be compliant with the Blueprint.

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

Commentary:

Judicial independence is a basic 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.[9] 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-800-171r1.

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

[9] "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.

2. POLICY

Policy 2a: Responsibility for Judicial Information security policy 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 a government entity.

Policy 2b: 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: A set of model policies governing information security and privacy should be officially adopted, approved and published by the Canadian Judicial Council, based on priorities identified in the Blueprint (Access Policy 7).

3. GOVERNANCE

Policy 3: The security of Judicial 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 Judicial 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 Judicial Information, in accordance with the threat and risk assessment.

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

4. JITSO

Policy 4: 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 accountable to the judiciary, ideally exclusively so, 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.

5. AWARENESS AND TRAINING

Policy 5: Basic 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 users with access to Judicial Information.

Commentary:

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.

6. CLOUD MIGRATION

Policy 6a: Judicial Information may not be migrated to the cloud without the consent of the judiciary. As such, the judiciary must be included in negotiations for proposed cloud services including governance, operations, access controls, data location, and other security considerations. The security, privacy and integrity of Judicial 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 Judicial 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 Judicial Information to be managed.

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

7. DATA LOCATION

Policy 7: Judicial Information must be stored in a computing facility located within the geographic boundaries of Canada. Judicial 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:

Judicial Information 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.

Cross references: Treasury Board, Direction for Electronic Data Residency, IT Policy Implementation Notice 2017-02, https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html. 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.

8. COMPLIANCE

Policy 8a: 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 Judicial Information and Judicial Users, these must be done in compliance with the Monitoring Guidelines.

Policy 8b: In circumstances where Judicial 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 Judicial Information may be exempt from the search, review and disclosure processes.

Commentary:

Whether Judicial 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 Judicial 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).

Framework: 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).

9. PERSONNEL SECURITY

Policy 9a: 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 Judicial 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 Judicial Information. Procedures must exist to ensure the removal of access when an employee or contractor departs or transitions to a new role.

Policy 9b: Access to Judicial 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 Judicial Information is granted, a user must have at a minimum:

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

10. ACCESS CONTROL

Policy 10a: With respect to Judicial 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 10b: Judicial information systems containing "Personal" or "Individual" 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 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).

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

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

11. MONITORING

Policy 11a: 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 11b: Analytical tools may not be applied to Judicial Information (including information that has been anonymized) 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.[11] Judicial research may require access to blocked websites. For a model Acceptable Use Policy, see Appendix 4 below.

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).

12. MOBILE DEVICE MANAGEMENT

Policy 12: Courts must implement a Blueprint-compliant policy for mobile devices and implement security protocols that allow for the wiping of data from lost or stolen devices.[12]

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.

[11] See ISO 27002, 12.4.1.

[12] See sample policy at Appendix 3. Even with effective remote wiping tools, if the device is not connected to the Internet or if it is placed in "airplane" mode it cannot be erased remotely.

- First, 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.
- Second, 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.
- Third, 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.
- Fourth, 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.

13. SOCIAL MEDIA

Policy 13: 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."[13] Policies and training should address all known risks.

14. INCIDENT MANAGEMENT AND REPORTING

Policy 14: 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:

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

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 Canadian Judicial Council Computer Monitoring Guidelines 2002 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.

15. CLASSIFICATION OF JUDICIAL INFORMATION

Policy 15a: Courts should adopt a classification scheme so that sensitive Judicial 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 15b: No Judicial Information may be published, shared, exchanged or provided to any third parties, including any government agency, except with prior written judicial approval and in accordance with applicable legislation.

Commentary:

The author of a document should be responsible for assigning the appropriate classification to information that he or she has created.

The following two-level classification scheme provides one very simple 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.

> **For Judicial Use Only** – All Judicial Information is by default classified as "For Judicial Use Only" and is therefore subject to the protections outlined in this Blueprint.
>
> **Protected** – This classification can be used for highly sensitive Judicial Information, for example: documents containing personal information that may relate to judges, to matters and parties; draft judgments, e-mails relating to judicial opinion and case law, and memoranda about issues affecting the judiciary.

Protected information would be subject to more stringent treatment, including special markings, encryption, and storage on designated devices.

The author is responsible for deciding when Judicial Information is no longer classified and may be released to non-judicial users. For example, when a draft judgment is finalized it may be released to the public in accordance with the judge's instructions.

Cross references: Asset Management ISO 27001:2013, A.8.

16. ENCRYPTION

Policy 16: The judiciary must be involved in the development of encryption policy and implementation, as they relate to confidentiality, integrity, non-repudiation and authentication of Judicial Information. Encryption policy and procedures should be consistent with the classification scheme for Judicial Information. Key management, including policies and procedures, must be in the hands of the judiciary.

Commentary:

The objective of this policy is to make encryption tools readily available to Judicial Users, manage the encryption process securely, and protect sensitive information from unauthorized access.

Software, standards and management protocols relating to the encryption of data through the use of digital certificates comprise what is known as PKI, or the Public Key Infrastructure.

A digital certificate, issued by a trusted third party, verifies the identity of a user and connects that user to a unique public key, which allows for the exchange and decryption of encrypted messages. To ensure complete independence, it is recommended that the certification authority for judicial users be a trusted third party independent not only of the judiciary but of the government.

The decision to encrypt data should be based on documented court security risk management decisions and the application of the Judicial Information classification scheme.

• Anyone using encryption on Judicial Information must be known to the judiciary and provide information about the product functionality.

• The JITSO should instruct all users in the use of encryption technology and should develop and document procedures for recovering encrypted information. The JITSO should also be responsible for monitoring all user requests for authentication.

Cross references: ISO 27001:2013A.10. ISO 27017:2015, s. 10, ISO 27002, 10.1.

17. PHYSICAL SECURITY

Policy 17: All processing facilities or equipment used for Judicial Information must be located in a physically secure environment, with access limited to authorized individuals. Physical security must be designed to protect Judicial 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.

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

18. INFORMATION SYSTEMS

Policy 18: The processes for acquisition, development and maintenance of court information systems must be designed and applied so as to safeguard the quality, integrity and long-term availability of Judicial Information and Court Information. Judicial Information should be subjected to additional protection over and above the security safeguards applied to Court Information.

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

Framework: Foundational Policy 10, Security Policy 5.

19. COMMUNICATIONS AND OPERATIONS

Policy 19a: 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 Judicial Information through any type of communication medium or technology.

Policy 19b: 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 synchronisation
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 Judicial 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.)

Framework: 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).

20. BUSINESS CONTINUITY

Policy 20: Courts must protect Judicial Information in the event of a catastrophe 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 network storage that is backed up at least daily. Effective provision must be made to facilitate back up of Judicial 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:[14]

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.

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.[15]

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

- ISO/IEC 27001 and 27002:2013
- Security and Privacy Controls for Information Systems and Organizations, NIST Special Publications SP800-53r5

Select standards for Canadian jurisdictions include:

- British Columbia Information Security Policy (July 2016) issued by the Office of the Government Chief Information Officer;
- Government of Ontario GO-ITS (General security requirements for the protection of the integrity, confidentiality and availability of Government of Ontario networks and computer systems.);
- Standard of Good Practice for Information Security (2016), published by the Information Security Forum (ISF), and used in New Brunswick.
- IT Risk Management guidance (see https://www.cse-cst.gc.ca/en/publication/list/IT-Risk-Management)

[14] For a basic guide, see https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-en.aspx, "A Guide to Business Continuity Planning", Public Safety Canada.

[15] http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf.

- ITSB 67 Cyber Security Considerations for Management - Guidance for the Government of Canada
- ITSE.10.033 IT Security Risk Management in the Government of Canada
- CLOUD (see https://www.cse-cst.gc.ca/en/publication/list/Cloud)
- ITSE.50.060 Cloud Security for the Government of Canada
- ITSB-105 Security Considerations for the Contracting of Public Cloud Computing Services

APPENDIX 1

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 2

GLOSSARY OF DEFINED TERMS AND ACRONYMS

Term	Meaning
Analytics	"The discovery and communication of meaningful patterns in data" - see http://en.wikipedia.org/wiki/Analytics.
Anonymization	The process of removing personal identifiers from collections of data.
Apps	Software applications that are downloaded for use on mobile devices.
Big data	Usually defined as so much data that it is impossible to handle without special software tools. A good overview is found here: http://www-01.ibm.com/software/data/bigdata/.
BYOD	Stands for "Bring your own device" a policy that allows users to access business networks using mobile devices belonging to them personally.
Cloud	"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." See NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
Cryptography	The science of encryption.
CSP	Cloud services provider
DDoS	Distributed denial-of-service; a kind of cyber-attack which overloads a website and prevents users from accessing it as a result
Encryption	A process that translates human-readable text into unreadable code for the purpose of securing information from unauthorized access.
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	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.
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.
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.

Term	Meaning
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.
Shared services	Shared services refers to the provision of a service by one part of an organization or group where that service had previously been found in more than one part of the organization or group. Thus the funding and resourcing of the service is shared and the providing department effectively becomes an internal service provider. Wikipedia, http://en.wikipedia.org/wiki/Shared_services.
SLA	Service level agreement. The SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the "level of service" defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. Wikipedia, http://en.wikipedia.org/wiki/Service-level_agreement.
TRA	Threat and Risk Assessment
Virtualization	"With virtualization, several operating systems can be run in parallel on a single central processing unit (CPU). This parallelism tends to reduce overhead costs and differs from multitasking, which involves running several programs on the same OS. Using virtualization, an enterprise can better manage updates and rapid changes to the operating system and applications without disrupting the user." Wikipedia, http://en.wikipedia.org/wiki/Virtualization
WiFi	Used interchangeably with WLAN, though technically it refers to a WLAN configured in accordance with a particular standard.
Wireless LAN (WLAN)	A local area network using radio frequency rather than wires to connect.

APPENDIX 3

EXAMPLE MOBILE DEVICE SECURITY POLICY FROM SOPHOS

Downloaded without modification from http://www.sophos.com/en-us/medialibrary/PDFs/other/Example%20Mobile%20Device%20Security%20Policy.docx.

Example Mobile Device Security Policy

Using this policy

One of the challenges facing IT departments today is securing both privately owned and corporate mobile devices, such as smartphones and tablet computers. This example policy

is intended to act as a guideline for organizations looking to implement or update their mobile device security policy.

Feel free to adapt this policy to suit your organization. Where required, adjust, remove or add information according to your needs and your attitude to risk. This is not a comprehensive policy but rather a pragmatic template intended to serve as the basis for your own policy.

Background to this policy

The most common challenge is that users do not recognize that mobile devices represent a threat to IT and data security. As a result they often do not apply the same security and data protection guidelines as they would on other devices such as desktop computers.

The second challenge is that when users provide their own devices they often give greater weight to their own rights on the device than to their employer's need to protect data.

This outline policy gives a framework for securing mobile devices and should be linked to other policies which support your organization's posture on IT and data security.

Example policy

1. Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals.

However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

<Company X> has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Scope

1. All mobile devices, whether owned by <Company X> or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.

2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by security management.

3. Policy

3.1 Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later. <add or remove as necessary>
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with <Company X>'s password policy. This password must not be the same as any other credentials used within the organization.
4. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

3.2 User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to <Company X> IT immediately.
3. If a user suspects that unauthorized access to company data has taken place via a mobile device they user must report the incident in alignment with <Company X>'s incident handling process
4. Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact <Company X> IT.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with <Company X>'s compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify <Company X> IT immediately.

11. (If applicable to your organization) Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

APPENDIX 4

MODEL ACCEPTABLE USE POLICY

The Canadian Judicial Council has drafted this Acceptable Use Policy as a model for courts. Any policy regarding acceptable use for Judicial Users must consider the principles of independence (institutional as well as individual) and the following issues:

1. Who sets the rules?
2. Who decides on exceptions?
3. How are behaviour and compliance monitored?
4. How is a breach of the policy investigated and reported?
5. How is non-compliance handled?

Purpose: To ensure that Judicial Users have uninterrupted access to a secure, private and reliable information system (the "Service"). The Policy is designed to be consistent with the principles of judicial independence and compliant with the Council's Monitoring Guidelines.

The following activities are generally prohibited for all users:

- Using the Service to run a private business.
- Attempting to access the account of another user
- Sharing passwords
- Reselling the Service to a third party
- Sending unsolicited bulk email
- Accessing blacklisted web sites*
- Downloading or installing unapproved software*
- Overburdening the Service (or the networks connected to the Service)*
- Engaging in, facilitating, or furthering unlawful conduct
- Damaging, disabling, or impairing the service
- Interfering with another's use and enjoyment of the Service

***Exceptions**. From time to time a Judicial User may require access to a blacklisted web site; may have a legitimate business reason to install unapproved software, or may need to download

or stream unusually large volumes of data. In those cases the [service provider] shall have a process for applying for an exception and reasonable approval of a work-around to accommodate the need.

Monitoring and Incident Response. The [service provider] has the right to monitor user and network activity in order to protect all users against prohibited activities. However, in accordance with the Monitoring Guidelines, "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."

Where the [service provider] has reason to believe that a Judicial User has committed a prohibited activity, it shall promptly disclose its findings to the judiciary before taking any other action.

Suspension. In consultation with the JITSO, the [service provider] may suspend a Judicial User's access to the Service if:

(1) The service is being used for a prohibited use

(2) The Service is being used to further a criminal or illegal purpose

Reinstatement. A user may be reinstated after consultations between the judiciary and the [service provider].