CJC
Canadian
Judicial Council

Blueprint
for the Security
# of Judicial Information

Fourth edition, 2013

Prepared by Martin Felsky, PhD, JD, for the Technology Subcommittee of the Administration of Justice Committee of the Canadian Judicial Council, July 4, 2013.

TABLE OF CONTENTS

INTRODUCTION

The Blueprint is intended to serve several purposes. Its major 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.[1] 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.

[1] 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.

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[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.
- 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]

More recently, the Council adopted sixteen foundational policies relating to court information governance, as set out in the *Court Information Management Policy Framework to Accommodate the Digital Environment,* ("Framework Report").[4] The Framework Report 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

Though the statutory mandate of the Council is limited to federally-appointed judges, those judges often share IT resources with their provincially-appointed counterparts. For that reason alone, collaboration on the development of security policies is encouraged. The Blueprint applies to any computer system

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

[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.

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

which is used for Judicial Information. This would include home computers, some peripherals, data communication networks and mobile devices.

The Framework Report 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" will be used to include Judicial Officers and the broader range of individuals who have access to 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. [5]

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.[6]

Examples of Judicial Information would include[7]:

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

[6] Framework Report: "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]."

[7] Examples taken from Framework Report, page 33.

- 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
- All 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 as defined exists and must be protected not only on active servers, devices and storage media but in archival, imaged and backup systems as well.

Security of IT systems 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 an IT department. In that respect, the Blueprint does not cover every aspect of security administration. Nor does the Blueprint discuss security relating to security of 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 enhance existing policies and programs within government, and to supersede them *only if they conflict with or are less stringent than those proposed here*. To that extent, the Blueprint is intended to seamlessly co-exist with worldwide IT security standards, guidelines and best practices such as ISO 27002, the ISACA CobiT Framework[8], Information Security Forum, "Standard of Good Practice[9]," and various published and draft NIST works such as 800-53 ("Recommended Security Controls for Federal Information Systems") and 800-39, ("Managing Risk from Information Systems") among many others.[10] For a helpful and detailed examination of the differences between the Canadian

[8] "Control Objectives for Information and Related Technologies", www.isaca.org.

[9] https://www.isfsecuritystandard.com/SOGP07/index.htm.

[10] National Institute of Standards and Technology, http://csrc.nist.gov/. One of the original resources upon which the original Blueprint was based is the Communications Security Establishment, *Canadian Handbook on Information Technology Security*, March 1998 ("CSE Handbook").

Government MITS requirements and ISO 27001 see “Improving the Management of Information Security in Canadian Government Departments” by Ken Fogalin, 2009.[11]

COMPLIANCE

IT security policies and standards are meant to be mandatory. Universal compliance with security requirements protects all users in any organization. But in at least one vital respect, judges are not like other users – they are not subject to supervision or disciplinary procedures by the organization that supports their IT requirements.

The very idea that policies or procedures are expected to be mandatory causes some concern among many judges. However, without universal compliance the safety and integrity of all Judicial Information is at risk. Since the Council proposes that all policies and standards affecting judges must emanate from or be approved by judges, that compliance, even without any direct enforcement mechanism, could be more readily obtained.

The fact is that if any one user – judge or otherwise – fails to adhere to an appropriate security standard, then the entire network, and the security of the information of all judges and other users on the network, could be compromised. For example, if a single judge were to choose a weak password, or fail to properly encrypt a sensitive e-mail attachment (such as a draft judgment), an unauthorized outsider could gain access not only to the files of the imprudent judge, but to those of judges who may meticulously maintain on their own account the highest level of security preparedness. For this reason, the Council encourages all judges and other users of court systems to adopt the policies and practices set out here, not only in the interests of the judicial system, but to the benefit of those third parties whose information requires special protection under the law.

In some cases where provincial authorities have asked judges to comply with government security rules or acceptable use policies, judges have raised objections with respect to a potential compromise of their independence. It is hoped that judges will have an easier time conforming to the recommendations made in the Blueprint, as this is a document written by judges, for judges.

NOTE TO THE FOURTH EDITION

In addition to ensuring that the Blueprint is in keeping with the latest technological innovations, as well as recent best practices for information security management, the Technology Subcommittee of the Administration of Justice Committee of the Canadian Judicial Council agreed to restructure the document as a bright line minimum required standard, as opposed to a general guideline. This new approach is designed to assist the judiciary across the country in negotiating with their respective court administrations to ensure that judicial independence and privacy are always taken into account when security systems are designed and implemented.

[11] See http://www.sans.org/reading_room/whitepapers/leadership/improving_the_management_of_information_security_in_canadian_government_departments_33063.

This fourth edition of the Blueprint is therefore not a routine update. Significant developments in technology have moved the debate about judicial independence to the forefront, and have prompted the judiciary to take a serious look at a wide range of information governance issues including security.

Even while addressing new topics and introducing new policies, the Blueprint document has been shortened and simplified to make it easier to read, and its sections have been aligned with those of ISO 27002, the leading global information security standard, to make it easier to implement. There is much less commentary than before: emphasis is now on the expanding role of the judiciary in crafting policy and auditing compliance, and not on the technical details of implementation.

In this edition, technical detail is avoided for three reasons: first, because specific instructions become outdated very quickly, and should not be used as a baseline for security when newer and better methods become available; second, instructions that are too specific only apply to certain court installations and are not useful to others; and third, it is not necessary or helpful for the Blueprint to duplicate the very detailed and highly technical standards and guidelines already used by governments across the country. The real value and importance of the Blueprint is its focus on the judiciary as information owners, and how the principles of Judicial Independence must be respected as IT security is planned and implemented throughout the justice system.

Since the third edition of 2009, four technologies in particular have had a huge impact on information security thinking and have raised new concerns about cybersecurity worldwide. The four technology trends with the greatest impact on information security practices are:

1 Cloud computing
2 Social media
3 Mobile devices
4 Big data

Each of these will now be discussed in turn.

1. CLOUD COMPUTING

Cloud computing has raised significant concerns among the judiciary specifically with respect to judicial independence. As readers of the Blueprint are aware, it is the unique feature of judicial independence that differentiates the Blueprint from other information security policy documents, and which has made the Blueprint an indispensable resource for many Canadian judges and court administrators.

Cloud computing is rapidly gaining popularity though the technology is still relatively new. While the definition of cloud computing is somewhat nebulous it usually involves computing resources available to users off-site and through the magic of virtualization, shared with other users.[12] Cloud computing allows users in different organizations to share hardware, network services and even software in the same data

[12] Virtualization is a technology that allows multiple instances of an operating system to be installed on a single physical server or cluster of servers. This allows for the efficient consolidation of server hardware while maintaining the same segregation of users and applications previously only available through the deployment of separate physical servers.

centre, but with each organization independently managing its own user access and information independently. This contrasts with traditional architecture 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 power that they need, leaving the administration of the technology to their provider.

Cloud computing is a technology, not necessarily a business. For that reason, organizations can establish cloud computing infrastructures internally ("private cloud"), if they prefer not to outsource the provision of computing and network services. Even if the business is not outsourced, huge savings are available through centralization, consolidation and virtualization of physical resources, as well as the centralization of regional overlapping IT management and support infrastructures.

Governments across the country are no less aware of the benefits of consolidating hardware and IT support, security and other management services, and have been joining the global trend. The savings are especially attractive for court administration services, given the fact that courts are spread out throughout the country in numerous, sometimes very small and under-resourced jurisdictions.

Another aspect of cloud computing relevant to the security of judicial information can be called the "personal" cloud. Individuals using applications on mobile devices may be required, or have the option, to backup their data "in the cloud" or synchronize with their other devices using a cloud-based third party. While these services are very convenient and offer a measure of comfort (mobile data backup), there is a risk that Judicial Information can be compromised, because it is being entrusted into the hands of unknown third parties, often based outside the country. The data may not be covered by privacy laws or any enforceable contractual protections.

INFORMATION SECURITY CONCERNS

Together with the efficiencies and cost savings of cloud computing usually come increased physical security. This is true because protecting one large data centre is much less costly than protecting a dozen or a hundred spread out across court districts. The concerns about cloud computing for courts is not so much the physical security, but the organizational security, the personnel security, and the IT security. The trend to shared services, for example, which may be one step on the way to cloud computing, is a major concern for the judiciary because it raises questions as to the accountability, segregation, ownership, access to, custody and control of judicial data.[13]

Consolidation from the government's perspective leads to greater control over IT spending and IT management. From the perspective of the judiciary, however, consolidation of network, computing and

[13] As the NIST Special Publication 800-146 expresses it, "When an organization subscribes to a cloud, all the data generated and processed will physically reside in premises owned and operated by a provider. In this context, the fundamental issue is whether a consumer can obtain an assurance that a provider is implementing the same or equivalent controls as to what the consumer would have implemented."

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 take an active role in specifying how it wants Judicial Information to be managed by its service provider. For that reason, this version of the Blueprint provides at Appendix 4 an outline of a service level agreement that could be used as a model in any jurisdiction. Certain risks of cloud services are specifically addressed in Policy 9e.

2. SOCIAL MEDIA

The rapid growth and ubiquity of social media have had a major impact on thinking about open courts. Because the use of social media such as micro-blogging during a trial is not strictly speaking a security issue, nor does it necessarily relate to Judicial Information, it is beyond the scope of the Blueprint. Some courts have drafted policies governing the use of social media in court. Concerns about social media also relate to the use of social media by Judicial Officers and Judicial Users. For example, when court administrators engage in social media activity, do they represent the court? If judges join social media networks, how should they behave, and is it acceptable to "connect" with lawyers or members of the public? Again, while these questions are outside the scope of the Blueprint, they have prompted the Council to ask some hard questions about the relationship between a fair trial and the pervasiveness of social media. Certain risks of social media are addressed in Policies 2b and 8e.

3. MOBILE DEVICES

Mobile devices are getting smarter and more convenient. Smartphones are capable of running any one of hundreds of thousands of available software "apps", and the sale of tablets is expected to outstrip the sale of laptops imminently. These devices, whether provided by the court -- or, as is the dominant trend -- purchased by users themselves, raise several security red flags.

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, or built and configured with the same security capabilities in mind.

Second, mobile devices are computers that can generate, manipulate and store data. However, password protection on these devices can be weak, encryption options may be limited or non-existent, and the devices are often 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, even in some cases when the device is turned off. 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.

Although beyond the scope of the Blueprint, mobile devices also present real challenges in the event of an investigation or electronic discovery project.

Whether issued by court administration, used as part of an official “bring your own device” (BYOD) policy, or used outside of the court’s security program entirely, mobile devices are challenging traditional approaches to information security. Some aspects of mobile security are specifically addressed in Policy 8f.

4. BIG DATA

“Big data” is the term used to describe the enormous and rapidly growing volume of digital information created and stored by public and private organizations. Big data can be a big problem and a big opportunity for any organization. For the limited purposes of the Blueprint, big data raises privacy issues not only for Judicial Users but for all stakeholders in the justice system. Courts encounter big data issues, for example, when converting old printed law reports to digital versions for access on CanLII. What was once locked in paper files is now searchable online. Personal information about litigants, relatively difficult to access by the operation of “practical obscurity,” becomes readily accessible to anyone with a smartphone. While in principle this information was always open to the public, early decisions were never handed down with the expectation of global publication and instant public access.

To help organizations organize and mine the vast quantities of structured and unstructured data they now collect, a new breed of powerful tools are being used by governments and large private organizations called “analytics.” When applied to existing and future internal court systems, these processes and programs can shed very useful light on all sorts of interesting data, for example statistics on court filings, delays and dispute outcomes. At the same time, information that was never thought to be available can be extracted, combined, collated and presented in reports.

As courts continue to implement automated case management tools, e-filing, e-trials and similar technologies, the benefits and risks of big data can emerge very quickly. In addition to concerns about privacy, there are concerns about ownership, accuracy of the information generated by analytics, and the uses to which it may be put. Certain risks of big data are addressed in Policy 10b.

FRAMEWORK REPORT

The Framework Report 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 Report, to which the reader of the Blueprint should refer.[14]

BLUEPRINT STRUCTURE

When the first *Blueprint* was envisioned more than a dozen years ago, it was important to provide not just bare policies, but explanatory notes to raise the level of awareness as to various basic aspects of information security. Since then, the qualifications and skill sets of government IT staff have improved, and security is taken much more seriously by governments across the country. This revision tries to eliminate overlap with well-known industry standards such as ISO 27002, as well as many detailed standards that are implemented government-wide, such as:

- British Columbia Information Security Policy (October 2012) issued by the Office of the Government Chief Information Officer;
- Government of Ontario IT Standards, for example 25.18 “Physical Security Requirements for Data Centres”;
- *Standard of Good Practice for Information Security*, published by the Information Security Forum (ISF), and used in New Brunswick.

Today what is important for the Blueprint is not to repeat the well-worn basics of IT security, but to highlight the unique nature of Judicial Information and guide those responsible for implementing policy as to the unique requirements of Judicial Users.

To make it easier to integrate Blueprint policies into existing government policies and standards, this edition of the Blueprint has been reorganized to more closely match the structure of ISO/IEC 27002. The following table is a concordance of policies[15]:

ISO 27002 Chapter	Blueprint 4th edition 2013	Blueprint 3d edition 2009
	1. Judicial Independence	10. Judicial Independence
4. Risk assessment	4. Risk assessment	4. Threat and Risk Assessment
5. Security Policy	2. Policy	2. Policy and Planning
6. Organization of Information Security	3. Organization of Information Security	1. Judicial IT Security officer
7. Asset management	5. Asset Management	7. Classification of Judicial Information
8. Human resources	6. Human Resources	3. Security Awareness and Education
9. Physical and environmental	7. Physical Security	6. Physical Security
10. Communications and Operations	8. Communications and Operations	13. Intrusion Detection System systems 14. Protection against malicious

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

[15] Some 3d edition Blueprint policies may appear more than once because they are relevant to more than one ISO chapter.

ISO 27002 Chapter	Blueprint 4th edition 2013	Blueprint 3d edition 2009
		code, spam and related threats
11. Access control	9. Access Control	8. Controlling access to court systems 9. Remote access control and wireless networks 10. Judicial Independence 12. Firewalls
12. Information Systems Acquisition, Development and Maintenance	10. Information Systems	7. Classification of Judicial Information 11. Encryption
13. Incident management	11. Incident Management	
14. Business continuity	12. Business Continuity	5. Backup and business continuity planning
15. Compliance	13. Compliance	Introduction

POLICIES[16]

1. JUDICIAL INDEPENDENCE

Policy 1a: The principles of judicial independence must be incorporated by design into any information system that includes Judicial Information or serves Judicial Users.

Policy 1b: All judiciary, court staff, and court communications will use a common Internet domain that is distinct from the government domain (Framework Foundational Policy 8).

2. POLICY

Policy 2a: The judiciary is responsible for making and approving security policies that affect Judicial Users or Judicial Information. All court security policies are to be interpreted and applied in accordance with the Council's Monitoring Guidelines.

Policy 2b: In order to safeguard the reputation of the justice system and balance the principles of open court with fair trials, the judiciary must set policies and codes of conduct for social media use by Judicial Users.

Policy 2c: Information Management Policies will be published on the Court web site (Framework Access Policy 7).

3. ORGANIZATION OF INFORMATION SECURITY

[16] There are 13 categories of policies, and a total of 45 individual policies set out in the Blueprint.

Policy 3a: 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.

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 (Policy 4).

Policy 3b: Every jurisdiction must ensure that a Judicial IT Security Officer who is accountable to the judiciary be appointed to oversee the management of court information technology security operations.

Policy 3c: 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 (Framework Privacy Policy 3).

4. RISK ASSESSMENT

Policy 4: Every court must plan and conduct a regular threat and risk assessment ("TRA") in collaboration with the judiciary. The level of detail required in a TRA, its scope, and the time interval between assessments may vary from one court to another depending on the circumstances.

5. ASSET MANAGEMENT

Policy 5a: All court information, including all the equipment used to manage it, is considered an asset and as such must be inventoried and assigned to owners and custodians.

Policy 5b: All equipment, hardware or media used to store Judicial Information must be disposed of in a secure manner.

Policy 5c: Irrespective of who has custody, the judiciary always has ownership of Judicial Information.

Policy 5d: Courts should adopt a classification scheme so that sensitive Judicial Information may be designated for isolation.

Commentary: When we think of assets we generally refer to servers, laptops, and all the other hardware components that make up a complex information system. Printers, scanners, monitors, and a variety of peripheral equipment that exists in the data centre. Because so many of these physical assets can contain or store Judicial Information, and because mobile gear is so easy to lose or misplace, it is important that all physical equipment to be inventoried, labeled, tracked and physically secured (or secured by encryption if possible).

It can be more difficult to conceive of information itself as an asset. In fact, treating information as an asset makes it easier to understand why it is so important to protect it. If the courts were stockpiling diamonds, there would be no question about spending appropriate amounts of money to safeguard those diamonds, which have a value that can be assigned in dollar amounts. While it is probably impossible to assign a dollar value to Judicial Information, is very clear that without information the court system would simply be inoperable.

Once we recognize information as an asset, albeit an invisible one, we need to inventory it, label it, track and secure it just as we do the equipment which is more visible and more susceptible to physical safeguarding. We have an additional task which is made more difficult by the nature of information: that is ownership. For every category of information in the court system, including databases, software, court records, pleadings, and so forth, it is important to assign ownership.

Policy 5b is not intended as a proclamation of legal ownership. Rather, “ownership” is used in the sense of taking responsibility for something. Legal wrangling about property rights, if these exist at all, is extraneous to our purposes here. Nothing in this policy prevents, where appropriate, joint ownership where information may be classified as both Judicial Information and non-judicial court information.

In some cases the “isolation” of sensitive Judicial Information referred to in Policy 5d may involve using systems completely outside of the court, such as JUDICOM.

6. HUMAN RESOURCES

Policy 6a: 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.

Policy 6b: No-one should have user-level access to Judicial Information unless they 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 (“Oaths of confidentiality will be contained in engagement contracts for employees, consultants and contractors to prevent inappropriate disclosure of sensitive Court Information” Framework Security Policy 2)

Policy 6c: No-one should have administrative-level access to Judicial Information unless they meet the requirements of Policy 6b and have been granted government security clearance at a level corresponding with their role.

7. PHYSICAL SECURITY

Policy 7a: All processing facilities or equipment used for Judicial Information must be located in a physically secure environment, with access limited to authorized individuals.

Policy 7b: Strong measures must be taken to physically protect network and power cabling that supplies processing facilities.

Policy 7c: Physical security must be designed to protect Judicial Information from natural disasters or human threats, consistent with the threat and risk assessment.

Policy 7d: Only authorized users may remove equipment that contains or accesses Judicial Information from a secure environment.

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 IT building 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, and government departments, agencies and tribunals.

8. COMMUNICATIONS AND OPERATIONS

Policy 8a: 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 8b: 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 8c: Courts are responsible for implementing controls to protect against malicious code, denial of service attacks and similar external threats.

Policy 8d: Whenever a third party provides any services related to Judicial Information, compliance with the Blueprint is required by agreement and must be monitored.

Policy 8e: 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.

Policy 8f: 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.[17]

Policy 8g: 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 (Framework Foundational policy 4).

Commentary: Operational controls usually address such fundamental aspects of court business as:

- proper documentation of all normal and emergency court functions
- procedures for change management
- segregation of duties
- system capacity and resource planning
- backup and restoration policy and procedures
- encryption infrastructure, tools, processes and training
- media handling, including handling of removable media and secure disposal of all computer equipment and media
- system monitoring, log management and auditing
- protection against malicious and mobile code
- protection against DoS (denial-of-service) and similar attacks
- security controls and procedures for physical media containing data in transit within and outside the court
- electronic commerce services including security of e-filing, online registries and publicly available information

9. ACCESS CONTROL

Policy 9a: With respect to Judicial Information, all access control decisions are the responsibility of the judiciary.

Policy 9b: The configuration of a court's access control systems must support the principle of judicial independence. Judicial Users should be provided with exclusive access to their own network resources unless it can be shown that network architecture, configuration, access controls, operational support and information classification schemes are sufficient to provide the highest level of confidence in the segregation between judicial and non-judicial information, and compliance with this Blueprint and the Council's Computer Monitoring Guidelines. ("Judicial Information must be protected from unauthorised

[17] 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.

access in accordance with the CJC's Blueprint for the Security of Judicial Information" Framework Security Policy 1.)

Policy 9c: All users accessing Judicial Information are responsible for using and managing their passwords in accordance with established policies.

Policy 9d: Judicial information systems containing "Personal" or "Individual" Judicial Information must be provisioned with an isolated, dedicated computing environment.

Policy 9e. Judicial Information may not be migrated to or transmitted through any commercial cloud services provider, whether public, private or hybrid, without the express written approval of the judiciary, and in that event, within subject to terms and conditions of a strict, Blueprint-compliant service level agreement.

Policy 9f: Information Exchange Protocols will be defined and negotiated with government agencies before court systems are designed and implemented. These protocols will be developed in line with the Fair Information Principles (Framework Access Policy 8).

Policy 9g: 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" Framework Security Policy 6)

Policy 9h: 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 (Framework Access Policy 5).

Commentary: This policy does not state 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.

Resources such as Guidelines for Securing Wireless Local Area Net*works (WLANs)* (NIST Special Publication 800-153), February 2012, can be helpful.[18] See also, *Cloud Computing Synopsis and Recommendations* (NIST Special Publications 800-146), May 2012.[19] For an introductory overview, see Steiner, *An Introduction To Securing a Cloud Environment*, June 2012, SANS Institute.[20]

10. INFORMATION SYSTEMS

Policy 10a: 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

[18] http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

[19] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

[20] http://www.sans.org/reading_room/whitepapers/cloud/introduction-securing-cloud-environment_34052.

Judicial Information and Court Information. (“Consistency, accuracy and promptness of Court Information and Judicial information is an essential goal of the system” Framework Foundational Policy 10.)

Policy 10b: The application of analytical tools to Judicial Information must not be done without the advice and approval of the judiciary.

Policy 10c: Judicial Information should be subjected to additional protection over and above the security safeguards applied to Court Information (Framework Security Policy 5).

Commentary: “Additional protection” may include, for example, data encryption policies.

11. INCIDENT MANAGEMENT

Policy 11: 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.

Every court must have in place a protocol for reporting of security incidents relating to or involving Judicial Users and/or Judicial Information to ensure that the principles of judicial independence are respected.

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.”

12. BUSINESS CONTINUITY

Policy 12: 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.

Commentary: A business continuity plan (BCP) should be based on the TRA and should include a process for regular maintenance, including training, testing, and updates. All business continuity plans must respect information security protocols. The elements of a simple business continuity plan would include:[21]

1 Governance

[21] See http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx, A Guide to Business Continuity Planning, Public Safety Canada.

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

13. COMPLIANCE

Policy 13a: All court information policies, procedures and practices must comply with applicable laws, regulations and valid contractual requirements.

Policy 13b: All court operations must be carried out in compliance with applicable information security policies including the Blueprint.

Policy 13c: Access to and use of compliance audit tools must be limited to a small number of authorized individuals only.

Policy 13d: Audit logs will be closely monitored to clearly identify which users have access to Court Information at any point in time (Framework Security Policy 3).

Policy 13e: Compliance with the above policies must be independently audited on a regular basis in accordance with the TRA. Where audits are performed on Judicial Information and Judicial Users, these must be done in compliance with the CJC Monitoring Guidelines.

KEY REFERENCES

- ISO/IEC 27002:2005
- NIST Special Publications such as 800-53 ("Recommended Security Controls for Federal Information Systems") and 800-39, ("Managing Risk from Information Systems")
- "Improving the Management of Information Security in Canadian Government Departments" by Ken Fogalin, 2009
- The Information Security Guide: Effective Practices and Solutions for Higher Education, published by the Higher Education Information Security Council.
- SANS Information Security Reading Room: http://www.sans.org/reading_room/

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 employees to access business networks using personal mobile devices belonging to them personally.
Cloud (see also Private Cloud and Hybrid 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
Hybrid cloud, see also Cloud and Private Cloud	A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms. http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud
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
IT	Information Technology
ITS	Information Technology Security
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.
Micro-blogging	Real-time publishing to the web short messages such as Tweets (on Twitter) or status updates (on Facebook) or any other social media network.
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.
Private cloud (see also Cloud and Hybrid Cloud)	"The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department." What is Private Cloud? Webopedia, http://www.webopedia.com/TERM/P/private_cloud.html
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.
Smartphone	A cellular telephone endowed with a screen and keyboard and sufficient computing power to run a variety of applications including a web browser.
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 may 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

JUDICIAL INFORMATION SLA OUTLINE OF TERMS

TERM (With Blueprint Policy Cross-Reference)	COVERS
Relationship between the parties	No partnership No assignment or subcontracting without judicial consent Where subcontracting occurs, all the terms of SLA must must be applied in the subcontract No conflict of interest permitted
Retainer	General agreement or understanding to provide service Operation of the system Access to the system and data General standard of service
Judicial Independence (Policy 1)	Framework Report, Blueprint and Monitoring Guidelines override inconsistent provisions in any other applicable IT security standard
Ownership (Policy 5)	Ownership of data Use and access restrictions Data to be stored and transported only in approved locations Data to remain in Canada unless otherwise agreed Isolation of data includes backups
Governance (Policy 3)	Joint Policy and Management Committee Incident Reporting Notice re lawful access Reporting requirements Compliance and Audit Dispute resolution
Service Levels	Scope Roles and responsibilities Hours of service Availability and maintenance End-user support
Security	Compliance with security policies (Policy 2) Asset Management (Policy 5) Human Resources (Policy 6) Physical security (Policy 7)

TERM (With Blueprint Policy Cross-Reference)	COVERS
	Communications and operations security (Policy 8) Access control (Policy 9) Information systems (Policy 10) Incident management (Policy 11) Business continuity (policy 12) Compliance (Policy 13)