Canadian Judicial Council

Blueprint for the Security of Judicial Information

Second edition, 2006

Revised 2006-09-28

Prepared by the Computer Security Subcommittee of the Judges Technology Advisory Committee

Contents

Executive Summary

1. This Blueprint is intended to serve several purposes. Its major objective is to provide guidelines to improve the security, accessibility and integrity of computer systems containing judicial information. Another purpose of the Blueprint 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 judicial needs into account.

2. The Canadian Judicial Council ("the Council") is concerned that the level of security provided for judicial information across Canada is uneven and inconsistent from jurisdiction to jurisdiction. The security of judicial information should be standardized as much as possible among all courts. Best practices should be determined and implemented in all cases.

3. The Council is also concerned that all too often, judges are not involved in a policy-making role. The Council would like to ensure that 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.[1]

4. The Blueprint applies to any computer system in which judicial information (as defined in the Blueprint) is created, stored or transmitted. This would include home computers, portable devices and peripherals if they contain judicial information.

5. The Council recognizes that some courts in Canada have sophisticated IT security policies and management programs in place. The Blueprint is designed to enhance those policies and programs, and to supersede them only if they conflict with or are less stringent than those proposed here. The Blueprint is also not intended to relieve courts from their individual responsibilities for undertaking threat and risk assessments based on their own unique environment.

---

[1] In September 2002, the Council's Special Committee on Future Directions published a report entitled "The Way Forward," which recommends that the Council assume a leadership role in the use of information technology in superior courts. See the Council's website, www.cjc-ccm.gc.ca.

6. 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 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.

7. The Blueprint sets out sixteen high-level policies that courts are encouraged to implement. A discussion follows each policy statement, together with a series of model guidelines to illustrate the policy. The document is not intended to be a technical manual, though there are references throughout the Blueprint to publications that do adopt a more technical approach. Rather, the intention is to educate judges and provide a foundation for each court upon which effective security measures can be built.

8. The Blueprint is divided into three sections corresponding to three types of security safeguards. The first group of policies has to do with management of IT security:

Policy 1: 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 2: Information technology security planning and policy for the protection of judicial information are judicial functions. The judiciary must take responsibility for making policies that affect judicial users or the manner in which they perform their duties. All court security policies are to be interpreted and applied in accordance with the Council's Monitoring Guidelines.

Policy 3: Courts must provide all users with ongoing awareness training and materials on IT Security, and all IT staff working with judicial information must be provided with mandatory in depth IT Security education.

Policy 4: Every court must plan and conduct a regular threat and risk assessment ("TRA"). The level of detail required in a TRA, its scope, and the time interval between assessments will vary depending on the relevant level of risk.

9. The main recommendation here is that each jurisdiction appoint a Judicial IT Security Officer, whose qualifications and duties are set out in the Blueprint. The Judicial IT Security Officer should be an IT specialist with technical experience and knowledge of security protocols appropriate to the size and sophistication of the court's computer system. This requires a management-level position with the individual capable of representing the judiciary with respect to IT security and reporting to the Chief Justice or Chief Judge.

10. The Judicial IT Security Officer would be responsible for providing independent advice to the judiciary on all matters relating to IT security and for performing regular security audits on IT systems containing judicial information. Further, the Judicial IT Security Officer would have overall responsibility for those IT security items that are primarily the responsibility of the judiciary, including policy development, risk assessment and ensuring compliance with policies and standards such as the Blueprint and ISO 17799.

11. The second section deals with operational safeguards including backup, physical security and a proposed classification scheme for judicial information:

Policy 5: 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, and stored locally, for example on notebook computers when travelling.

Policy 6: All critical network computing equipment should be located in a physically controlled environment, with access limited to personnel responsible for equipment administration and maintenance. The room must be equipped with proper environmental controls. If judicial users have notebook computers, then mechanisms such as laptop locks and alarms should be provided and used to reduce the risk of theft. Disk encryption is strongly encouraged for all notebooks. Controls such as physical access logs and video camera monitoring of network equipment should be implemented. Courts must ensure that when they dispose of any computer device or storage media (including backup tapes) no judicial information can be recovered.

Policy 7: Courts should adopt a classification scheme so that sensitive judicial information may be designated for special protection. Classified information must only be disclosed to those who have a need to know it.

12. According to the classification scheme, sensitive information should be identified either as “For Judicial Use Only” or “Protected.” Information so classified would be subject to special procedures to safeguard its confidentiality.

13. The last substantive section sets out policies respecting technical safeguards such as control systems for local and remote access, encryption, firewalls, intrusion and virus detection systems:

Policy 8: Courts must implement robust system access controls to ensure that only authorized users have access to any court system, and that their level of access corresponds to their security clearance and the court’s information classification scheme. Access rights to classified judicial information must be determined by the judiciary.

Policy 9: Special measures must be taken to ensure the security and privacy of all remote access connections and wireless networking.

Policy 10: 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 CJC Monitoring Guidelines.

Policy 11: Courts must make up-to-date encryption technology readily available to judicial users for the storage and transmission of classified judicial information on networks, desktops and notebooks.

Policy 12: All court networks containing judicial information must be protected from outside networks including the Internet with appropriate firewall technology that is effectively administered. All connections from a court’s network to external networks must pass through approved firewalls.

Policy 13: Courts must establish 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 Judicial IT Security Officer. When recommended in the TRA, courts should install network and host-based (or integrated) intrusion detection systems for real-time and automatic intrusion notification.

Policy 14: All court systems must employ industry-standard software to provide real-time detection and protection against malicious code, spam and related threats.

Policy 15: Such protective systems must be configured wherever possible on firewalls, servers, local workstations, notebooks, portable devices and home computers that contain or access judicial information.

Policy 16: All users must be trained in best practices for reducing the threat of malicious code, spam, and related threats.

14. One of the key aspects of this section is the discussion of judicial independence in Policy 10. The Policy assumes that only judicial users will have access to systems containing judicial information unless effective operational and technical steps are taken to ensure effective segregation.

15. The Council's Monitoring Guidelines, which set out the Council's views on how the monitoring of judicial computer activity should be restricted, are included with the Blueprint as Appendix 2. The Council's Model Judicial Acceptable Use Policy for Computer Technology is included as Appendix 6.

Introduction

16. This Blueprint is intended to serve several purposes. Its major objective is to provide guidelines to improve the security, accessibility and integrity of computer systems containing judicial information. Another purpose of the Blueprint 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 judicial needs into account.

17. The Canadian Judicial Council ("the Council") is concerned that the level of security provided for judicial information across Canada is uneven and inconsistent from jurisdiction to jurisdiction. The security of judicial information should be standardized as much as possible among all courts. Best practices should be determined and implemented in all cases.

18. The Council is also concerned that all too often, judges are not involved in a policy-making role. The Council would like to ensure that 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.

19. 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.

20. 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 and non-judicial users to preserve the independence of the judiciary.

21. The Canadian Judicial Council is acting 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]

22. The Blueprint is one part of the Council's approach to the security of judicial information.[4] The other components include:

    - Computer Monitoring Guidelines (2002) (Appendix 2)
    - Model Protocol for Court Technology Committees (2004) (Appendix 3)
    - "Ten Things Judges Can Do Now to Improve the Security of Judicial Data" (Second edition, 2006) (Appendix 4)

---

2 See Appendix 1. The 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.

4 For more information on The Council's information security initiatives, please see the Council's website at www.cjc-ccm.gc.ca.

- Initiatives with respect to the cleansing of metadata[5]
- Collaboration on ITS training with the Office of the Commissioner for Federal Judicial Affairs ("FJA") and the National Judicial Institute ("NJI")
- Model Judicial Acceptable Use Policy for Computer Technology (2003) (Appendix 6)

Scope and Application

23. 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. In addition, many judges use the resources of Judicom, the judicial communication network.[6]

24. The Blueprint applies to any computer system in which judicial information is created, accessed, stored or transmitted. This would include home computers, portable devices and peripherals if they contain judicial information.

25. "Judicial information" is information gathered, produced or used for judicial purposes, but does not include:

    (a) Court Services administrative policies and procedures and information specifically gathered or produced for the purposes of managing those court policies and procedures;

    (b) The chronological listing of court proceedings;

    (c) Exhibits, affidavits and other written evidence filed with the Court;

    (d) Documents, rulings, endorsements, orders, judgments and reasons for judgment that have been issued.

---

[5] See, for example, the article "The preparation of documents for electronic distribution," by Frédéric Pelletier and Daniel Poulin, http://www.lexum.umontreal.ca/ccc-ccr/guide/docs/distribution_en.html, which is drafted as a companion text to the "Canadian Guide to the Uniform Preparation of Judgments", adopted on September 2002 by the Canadian Judicial Council.

[6] Judicom was developed by the Office of the Commissioner for Federal Judicial Affairs

26. Judicial information is created by judges, including judicial officers such as Masters, Registrars, and Prothonotaries, and "judicial staff," including any employees or contractors who work on behalf of judges and whose work includes the handling of judicial information, such as executive officers, law clerks, law students, judicial clerks or assistants and judicial secretaries. Together, judges and judicial staff are referred to as "judicial users."

27. Security of IT systems is a complex field and the Blueprint cannot be comprehensive in its scope. Readers are advised to refer to standards, textbooks and papers noted in the references below. 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. For example, the Blueprint does not cover compliance with the laws of copyright or software licensing. (See ISO 17799, section 15.[7]) Nor does the Blueprint discuss security relating to IT support and operations, security of information that is not in digital form, security of telephone and fax communications, and the physical security of a courthouse. For an excellent discussion of IT operations security, see the CSE Handbook at chapter 14.[8] Voice and fax communications are covered in ISO 17799.

28. The Council recognizes that some courts in Canada have sophisticated IT security policies and management programs in place. The Blueprint is designed to enhance those policies and programs, 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 largely co-exist with the CSE Handbook (Canada), ISO 17799 (British/International), and the NIST Handbook[9] (USA).

---

7 All references are to ISO/IEC 17799:2005.

8 Communications Security Establishment, Canadian Handbook on Information Technology Security, March 1998 ("CSE Handbook"). Online copies are available free of charge in English at http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-e.html and in French at http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-f.html.

9 National Institute of Standards and Technology, US Department of Commerce, "An Introduction to Computer Security: the NIST Handbook." Available free of charge at http://csrc.nist.gov/publications/nistpubs/800-12/.

Compliance

29. 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.

30. 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.

31. 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.

32. 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, and ultimately sanctioned by the Canadian Judicial Council and other judicial organizations such as the Canadian Superior Court Judges Association and the Canadian Provincial Court Judges Association**.**

Structure

33. The body of the Blueprint loosely follows the structure of the CSE Handbook. However, unlike the CSE Handbook, the Blueprint sets out specific policies that are endorsed by the Council.

Policies are set out in boxes like this at the beginning of each section.

34. Following each policy statement is a discussion of the policy and in some cases model guidelines for each court in accordance with the results of its own risk assessment. Policies stated in the Blueprint are intended to be mandatory. Guidelines are not mandatory, but advisory in nature, and may need to be modified by each court to suit its particular circumstances.

35. To further assist judges and court administrators with the implementation of the Blueprint, there are extensive cross-references to the CSE Handbook, a comprehensive textbook by Charles Wood that provides hundreds of sample policies ("Wood"),[10] and ISO 17799.

36. With respect to IT security management, much of what applies to any government department or private sector organization is applicable to court settings. The same issues arise with respect to the management of information and users, operational and technical safeguards. To the extent these generic principles, policies and procedures are applicable in a court setting, the Council has relied on existing standards.

37. The Blueprint contains a glossary of terms and acronyms to assist the non-technical reader.

38. Another document that has been of great assistance to the Council is "Judicial Standards for Information Security and Protection," adopted for the Texas courts on December 14, 2001. The Texas report is accessible on the Web at http://www.courts.state.tx.us/jcit/index.asp. The Council would like to express its thanks to the Texas Judicial Committee on Information Technology ("JCIT") for its permission to borrow freely from that document. The Blueprint has been prepared by the Computer Security Subcommittee of the Judges Technology Advisory

---

[10] *Information Security Policies Made Easy*, by Charles Cresson Wood. Published by Information Shield, 2005. ISBN #1-881585-13-1. http://www.amazon.com/gp/product/1881585131/qid=1152494347/sr=1-11/ref=sr_1_11/102-6265597-7699340?s=books&v=glance&n=283155. All references are to the 10th edition.

Committee ("JTAC"). Members of the Subcommittee are: Justice Fran Kiteley (Chair of Subcommittee); Justice Adelle Fruman (Chair of JTAC); Associate Chief Justice Jeffrey Oliphant; Jennifer Jordan and Martin Felsky. The Subcommittee would like to thank Jeannie Thomas, former Executive Director of the Council, and Caroline Collard, Senior Advisor, for their invaluable assistance.

39. Early drafts of the Blueprint have benefited from consideration, comments and suggestions from various organizations, governments, courts and individuals, to whom the Council is grateful.

Note to the Second Edition

40. Once again the Computer Security Subcommittee of JTAC is indebted to those individuals at various courts across the country who were kind enough to provide feedback about the Blueprint. Current members of the Subcommittee are: Justice Margaret Larlee (Chair of JTAC), Justice Janet Simmons (Chair of Subcommittee), Associate Chief Justice Jeffrey Oliphant , Justice Adelle Fruman, Justice Eric Bowie, Jennifer Jordan and Martin Felsky.

Section One: Management Safeguards

41. All security efforts in any organization begin and end with management. For the courts, this most often means a collaborative approach in which judges set policy as it affects judicial information, and court administrators implement such policy through operational and technical safeguards. The Council believes that responsibility for the security of judicial information *at the policy level* is a judicial function and cannot be delegated to non-judges. This section of the Blueprint discusses the role of the Judicial IT Security Officer, Policy and Planning, Security Awareness and Education, and Threat and Risk Assessment.

1. Judicial IT Security Officer

Policy 1: 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.

Discussion

42. The designation of a Judicial IT Security Officer is intended to ensure that IT security is made a priority in the courts. This is one of the key recommendations (5d) approved by the Council on November 30, 2001 (See Appendix 1). It should also ensure that unique judicial circumstances and requirements form an integral part of IT security planning and system design. The Judicial IT Security Officer can act as a technical liaison with IT administration to enhance awareness of security among judicial users. The Council believes that at least one senior individual in every jurisdiction must be accountable exclusively to the judiciary for IT security of judicial information. (See ISO 17799, section 6.)

43. The main recommendation here is that each jurisdiction appoint a Judicial IT Security Officer, whose qualifications and duties are set out in the Blueprint. The Judicial IT Security Officer should be an IT specialist with technical experience and knowledge of security protocols appropriate to the size and sophistication of the court's computer system. This requires a management-level position with the individual capable of representing the judiciary with respect to IT security and reporting to the Chief Justice or Chief Judge.

44. The Judicial IT Security Officer would be responsible for providing independent advice to the judiciary on all matters relating to IT security and for performing regular security audits on IT systems containing judicial information. Further, the Judicial IT Security Officer would have overall responsibility for those IT security items that are primarily the responsibility of the judiciary, including policy development, risk assessment and ensuring compliance with policies and standards such as the Blueprint and ISO 17799.

45. Judges typically do not manage the information systems they use, but rather share network access to systems provided to them by a province. In the absence of their own judicially managed networks, judges must take ownership of security matters collaboratively with those organizations responsible for their management. The appointment of a Judicial IT Security Officer will facilitate that collaboration, providing judges with an appropriately trained adviser and representative.

46. Chapter 3 of the CSE Handbook describes different roles and responsibilities relating to organizational IT security. The Council recommends that while every court should have a designated Judicial IT Security Officer accountable to the judiciary, the job may be combined with other responsibilities provided they do not create conflicts. (It is not appropriate, for example, for the same individual to act as the Judicial IT Security Officer and an information security officer for court administration.) Like a Trial Coordinator, the Judicial IT Security Officer may be employed by the Attorney General but must report only to the Chief Justice or Judge. In general the following considerations should apply:

    - The Judicial IT Security Officer will deal primarily with policy issues, planning, standards, and the review or audit of security policy implementation. The role demands as much experience and knowledge on the security side as on the IT side.

    - The Judicial IT Security Officer should be accountable to the judiciary through the office of the Chief Justice or Chief Judge

    - The Judicial IT Security Officer should be sensitive to the issue of judicial independence

47. Job functions for the Judicial IT Security Officer may vary according to each court's IT environment, but the Council recommends the following core responsibilities:

    - Develop security policies for judicial approval;

    - Advise judges and administrators about IT security concerns relating to judicial information;

    - Generally oversee the adoption and implementation of this Blueprint and other relevant judicial IT security standards;

    - Coordinate security-related interaction within the court and between the court and other organizations such as the Council and the FJA, as well as with corresponding provincial and federal bodies responsible for IT security;

    - Design and provide, and coordinate with outside organizations (such as the NJI partnership with the FJA) IT security awareness and training programs for judicial users;

- Plan and supervise, in conjunction with the head of IT Operations, regular threat and risk assessments, audits and assurance testing for the court in accordance with judicial policies;
- Keep up to date about new information security risks and disseminate the information within the court;
- Oversee compliance with the Monitoring Guidelines;
- Validate and audit the court's metadata cleansing process;
- Arrange spot audits of court IT security;
- Draft rules for the Intrusion Detection System ("IDS") and its monitoring;
- Oversee the use of network-based IDS tools on a routine basis to ensure they are operating as intended;
- Establish relationships with incident response organizations and Judicial IT Security Officers in other courts, and share relevant threats, vulnerabilities, and incidents discovered;
- Oversee the approval process for new applications provided to or requested by judicial users;
- Ensure all users are properly instructed in the use of encryption technology;
- Oversee the implementation of encryption technology for judicial users.

2. Policy and Planning

Policy 2: Information technology security planning and policy for the protection of judicial information are judicial functions. The judiciary must take responsibility for making policies that affect judicial users or the manner in which they perform their duties. All court security policies are to be interpreted and applied in accordance with the Council's Monitoring Guidelines.

Discussion

48. Information security policy refers to the set of rules, protocols and practices courts and judges follow in order to manage and protect their information resources. See ISO 17799, section 5: "Security Policy."

49. Policies may be implemented in different ways. A good discussion of policies, including samples, is found in the CSE Handbook at chapter 5.

50. This Blueprint refers to three types of policies:

- Program policy sets a court's IT security program. It is high-level, comprehensive, and unlikely to need frequent updating. These policies apply irrespective of the nature of hardware or software implemented in the court, and are mandatory.

- System-specific policy includes rules and practices used to protect a particular information system. System-specific policy is limited to the system (or systems) affected and may change with changes in the system, its functionality, or its vulnerabilities. For example, courts that use the Novell Netware network operating system will require different rules from those using Microsoft Windows network operating systems.

- Issue-specific policy addresses issues of current relevance and concern to the court. Issue-specific policy statements are likely to be limited, particular, and rapidly changing. Their development may be triggered by a computer security incident. For example, a court's e-mail acceptable use policy is issue-specific.

Program Policy

51. Program policy as it relates to judges must exist within the framework of Canadian laws, regulations, and administrative policies. It must also be guided by the court's functions and organizational structure. Program policy development and promulgation is the responsibility of the Chief Justice or Chief Judge of each court.

The Judicial IT Security Officer would play a key role in policy development. Implementation can only be accomplished in consultation with the appropriate court administrative authority.

System-Specific Policy

52. Some courts are likely to have multiple sets of system-specific policies relating to security, from the very general (e.g., access control rules about who may have user accounts) to the very specific (e.g., system permissions reflecting segregation of duties among staff involved in handling case information). All system-specific policies must be consistent with program policy. Thorough technical knowledge of computer systems is often required in order to draft workable system-specific policy.

Issue-Specific Policy

53. Issue-specific policy statements can apply to a wide range of issues, including Internet access by users, installation of unauthorized software or equipment, and e-mail forwarding.[11] "Acceptable use policies" fall under this category. Courts must develop policies that apply to all users to the extent that systems containing judicial information are shared. However, only those policies approved by the judiciary may apply to judicial users. In December, 2003, the Executive Committee of the Canadian Judicial Council approved a "Model Judicial Acceptable Use Policy for Computer Technology", a copy of which is appended to this Blueprint as Appendix 6.

Guidelines for Policy Development

54. All ITS policies should be based on the court's threat risk assessment and generally include the following components:

    Purpose statement: The purpose statement explains why the policy is being established and its information technology security goals.

    Scope: The scope section will state which court resources – hardware, software (operating systems, applications, and communications), data, personnel, facilities, and peripheral equipment (including telecommunications) – are to be covered by the security policy.

---

[11] For example, courts may wish to advise judges not to set up their e-mail programs to automatically forward their secure messages to another address over an unencrypted connection, or courts may choose to disable the e-mail forwarding function.

Assignment of responsibilities: The program policy will document responsibility for information security program management, including the respective roles of the Chief Justice, Chief Judge, other judges, the Judicial IT Security Officer, judicial users, court administrators, and all non-judicial users.

Implementation: This section should describe how the court is going to oversee the implementation and enforcement of the information security policy.

Review date: The date at which the court intends to review the policy in question.

55. Policies must be drafted in a way that can be understood and appreciated by all users.

56. All security policies should be discussed with newly appointed judges and in new staff orientation, as well as in regular computer security awareness training.

57. Outside contractors, consultants and trainers should be required to sign security or confidentiality agreements to acknowledge that they are aware of their responsibilities and will abide by the court's security policies. The Blueprint does not address a situation where a court's entire IT function is outsourced to a third party, since this would require more complex attention to issues of public policy. See ISO 17799, section 6.2.

58. System-specific policies should be adopted for major programs such as operating systems, e-mail applications and office suites.

59. Issue-specific policies drafted by judges should be adopted regarding, for example, appropriate use of Internet and e-mail, installation of software, and personal use of computer resources. When judicial users log onto a system, a notice should be clearly displayed indicating that computer use is subject to these judge-made acceptable use policies.

60. Security policies should be reviewed at least annually to ensure that they are up to date and reflect the current computer system and court environment. An independent review is recommended from time to time. (See ISO 17799, section 15.)

3. Security Awareness and Education

Policy 3: Courts must provide all users with ongoing awareness training and materials on IT Security, and all IT staff working with judicial information must be provided with mandatory in depth IT Security education.

Discussion[12]

61. Security awareness, awareness training, and education are all necessary for the successful implementation of any information security program. These three elements are related, but they involve distinctly different levels of learning.

Security Awareness

62. The purpose of a security awareness program is to focus attention on security. Security awareness programs should be well established within the court. For example, documentation should be provided to all system users explaining the need for computer security and IT users' responsibilities for computer security.

63. Security awareness provides a baseline of security knowledge for all users, regardless of job duties or position. The base level of security awareness required of summer students or clerical assistants is the same as that needed by senior judges and court managers. IT security awareness programs should be tied directly to security policy development.

64. As part of his or her role in keeping up to date about new information security risks, the Judicial IT Security Officer should monitor appropriate sources, such as vendor and security sites, to ensure that users know how to detect or prevent IT system security incidents.

Awareness Training

65. Awareness training is geared to understanding the security aspects of the particular IT systems and applications used by an individual. For example, all users need to learn the security features of the word processing software resident on their respective systems, and how to back up their systems. All IT users also need to understand the security features of the local area network ("LAN") to which they are connected, as well as security issues related to connectivity to the Internet. There may be overlapping issues, but each system is a distinct entity that requires its own set of IT security measures. Security awareness training takes into account the uniqueness of each operating system and application.

---

[12] See Wood, 6.02, and ISO 17799, section 8.

66. Awareness training should be provided to all users of systems with access to judicial information. A sound practice is to conduct periodic (at least annual) refresher security awareness courses.

67. Formalized computer security awareness training should be provided to all new users at their orientation. Users should receive continuous security training in the form of bulletins, online resources, security alerts or tips, memos, and on-going annual training. All ITS training and materials should be coordinated to the extent possible and consistent with training and materials provided to judges through judicial organizations such as the Canadian Association of Provincial Court Judges and the National Judicial Institute/Federal Judicial Affairs Computer Education Partnership.

Education

68. Education differs from training in breadth and depth of knowledge, and skills acquired. Security education, including formal courses and certification programs, is most appropriate for a court's Judicial IT Security Officer and administrative IT personnel.

69. Network and firewall administrators and staff, and technical managers of networks should receive specific training on the operation of security products used in their environment to address IT security issues.

70. Network administrators should be required to pass a formal test on specific security issues related to the hardware and software systems for which they are responsible.

4. Threat and Risk Assessment

Policy 4: Every court must plan and conduct a regular threat and risk assessment ("TRA"). The level of detail required in a TRA, its scope, and the time interval between assessments will vary depending on the relevant level of risk.

Discussion

71. Security is always a compromise.[13] Security measures can be costly and inconvenient to implement, and it takes discipline within any organization to maintain a commitment to security. It is important that the measures taken to safeguard judicial information are responsive to relevant threats, and at the same time proportional to the risks.

72. Threats to the security, integrity and accessibility of judicial information come from various sources. These are sometimes categorized in the following way:

[13] "Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity." Harold F. Tipton and Micki Krause, *Handbook of Information Security Management*, http://www.cccure.org/Documents/HISM/003-006.html

Type of threat	Example
Natural threats, including fire, storms, floods, lightning, extreme temperature or other natural disasters	Power surge from lightning knocks out file server; "system is down" and no-one can log in to check e-mail, edit documents or perform any other computer system function.
Deliberate human threats from outsiders such as hackers, terrorists, organized crime, political activists and disgruntled litigants.	A teenager modifies online judgment text by hacking into the court's web server Contract IT staff gains access to draft judgments stored on a backup tape and posts it on a website Judge opens an e-mail message and launches a virus that shuts down all court e-mail service for 48 hours. A judge's laptop computer is stolen from the car while parked at a downtown office building. The computer contains personal information about a young offender, discovery transcripts which are the subject of a publication ban, as well as names, addresses, phone numbers and e-mail addresses of seven judges.
Deliberate or inadvertent human threats from system administrators and users	Disgruntled staff sends hate mail to politicians using a judge's e-mail address Judge inadvertently overwrites the final version of a 150-page judgment which was to be released that afternoon Three backup tapes are missing; critical court Scheduling information cannot be restored and must be re-calculated and entered.
Equipment failure, mechanical problem, software bug, or any other technical malfunction	Read-write head on server hard drive fails. System is down until a replacement can be installed and all backups restored.

73. Without effective safeguards, users are vulnerable to these and many other threats. Examples of poor information security practices include:

- Failure to identify and apply security related software patches in a timely manner
- Inadequately trained personnel responsible for network security
- Lack of computer security awareness throughout the court
- Unencrypted data being sent over public e-mail networks, for example MSN Hotmail
- Widespread use of weak passwords with no requirement for regular change
- Lack of policies and procedures related to judicial information security
- Inadequate physical security of computer resources, for example notebook computers
- Inadequate backup of judicial information, especially when located on personal computers and diskettes
- Lack of adequate virus protection

74. The basis for effective security planning is a threat and risk assessment ("TRA"). Threat and risk assessment is a formal process that should be done thoroughly and under the guidance of computer security experts.[14] Because the information technology environment is so different in every court, and concerns about security differ even among informed judges, a TRA must be performed by each court for its own circumstances. In general the phases of a TRA are as follows:

> **Asset Inventory**: Identify all the assets (including information, hardware and software) that require protection, whether located at the court or in the homes of users. In a court, information assets include not only judicial work product but information obtained from or about third parties (e.g.

[14] For assistance with the planning and implementation of a TRA, refer to an RCMP technical publication entitled "Guide to Threat and Risk Assessment for Information Technology", November 1994. To keep current, see the RCMP website at www.rcmp-grc.gc.ca and the CSE website, www.cse-cst.gc.ca. The CSE Handbook also provides an excellent discussion at chapter 7.

wiretap information or information about young offenders that may be subject to statutory security requirements).

Threat Assessment: For each asset, identify and assess all threats, including the source of the threat, the type of threat, the likelihood of the threat, and the *potential* impact of the threat.

Risk Assessment. Review the adequacy of existing safeguards to protect against the identified threats; in other words, assess where the court's security vulnerabilities are and the *actual* level of risk associated with each threat.

75. When all the steps of a TRA have been performed, a calculation results in which potential risks are evaluated. The following table presents a sample TRA calculation. From this calculation, courts can better determine the appropriate methods for better safeguarding judicial information.

Table Showing Sample TRA Calculation

Description of Threats	Potential Impact of threat (1-3)	Likelihood of threat materializing (1-3)	Risk Assessment (Potential Impact times Likelihood)
1. A hacker gains access to private internal resources.	High – 3	Medium – 2	6
2. A disgruntled user gains unauthorized access to information, which results in modification and or disclosure of sensitive information.	High – 3	High – 3	9
3. A virus infiltrates the court system and damages critical information.	Medium – 2	High – 3	6
4. A natural disaster results in loss of data and unavailability of the system.	High – 3	Medium – 2	6
5. A judge inadvertently damages critical information.	High – 3	Medium – 2	6
6. A hardware device malfunctions resulting in loss of data.	Medium – 2	Medium – 2	4

Section Two: Operational Safeguards

76. Operational safeguards support the implementation of security policies by dealing with user behaviour and the enforcement of best practices. There are many significant operational safeguards that are not covered in the Blueprint, as they are beyond the scope of direct judicial concern. In this section the Blueprint focuses on three key issues of particular concern to the judiciary: Backup, Physical Security, and the Classification of Judicial Information. For a much broader and informative look at operational safeguards generally, refer to the CSE Handbook Part III.

5. Backup and Business Continuity Planning

Policy 5: 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, and stored locally, for example on notebook computers when travelling.

Discussion[15]

77. ***Backup*** is a routine, regularly scheduled copying of critical system information, configuration and documents to ensure their availability in case the information on servers and workstations is lost. If a document is accidentally erased, or a program becomes corrupt, backup copies, which are usually saved to high-capacity magnetic tapes, can be restored to the server often in a matter of hours.

78. ***Business Continuity Planning*** provides protection in case of a system failure. For example, should a server be physically damaged or stolen, the court would need to be able to replace it quickly with a fully functional system to which applications and files could be restored. All courts should engage in a formal business continuity planning process.

79. In this section, various key elements of business continuity plans and backup procedures are set out.

Backup

80. Judicial information should be stored and backed up in such a way that the judicial users maintain exclusive access. These backups should then be archived in accordance with judicial policy. (See "Classification of Judicial Information," below.)

81. To facilitate backup of local workstations and notebooks, judicial information should be consistently stored in designated folders, for example "C:\Documents\Judicial\".

---

[15] See Wood, 8.04.01, 11, ISO 17799, sections 10 and 14.

82. If regularly scheduled network backup systems do not capture data from workstations, then judicial users should be periodically reminded to backup their systems by (a) copying judicial information to the designated network drive or (b) copying the contents of the designated local folder to reliable removable media such as a recordable CD or DVD.

83. Network backup tapes containing judicial information must be encrypted and stored offsite in a secure and trusted location. Backups of local workstations, if done separately, should be kept in a locked cabinet.

84. Routine backup and rotation procedures should include “full” weekly backups and nightly “incremental” backups for all computer and network operating systems, application programs, and data files. “Full” backups include copies of all current systems, applications, and files. “Incremental” backups only involve copying changes made to systems and files since the last backup.

85. All access to backup tapes must be subject to the Monitoring Guidelines (see Appendix 2).

86. There must be in place a procedure to regularly validate and verify that backup tapes are readable, especially prior to their being sent to the off-site storage facility.

87. All backup tapes must be accurately labeled.

88. One complete and regularly updated hardcopy inventory of all hardware and software should be maintained within the off-site tape storage facility (including operating systems, applications, purchased hardware and software, and both the vendor name and the court’s given name for each piece of hardware and software).

89. At least one complete hardcopy version of the most current Business Continuity Plan and any IT insurance coverage (for use in the event of a computer system loss) should also be kept in the off-site tape storage facility.

90. Hardcopy and digital versions of standard system configurations and documentation for all critical applications should be maintained at a physically secure off-site storage facility.

91. Tapes stored at the off-site storage facility must be kept in adequate dust free containers and be stored on their sides (especially 9-track tapes) in order to ensure that their data contents do not degrade or are lost completely.

92. Archival tapes (those kept for 2-3 years or more) must be checked annually for readability, and re-restored to newer media every few years, in order to maintain their capability to be restored (especially in the event new hardware or software make the old tapes unreadable due to new data text bit configurations).

93. The archiving of judicial information including electronic bench books must be done in accordance with policies determined by judges.

Business Continuity

94. The court should periodically update and regularly test its business continuity plans so that all systems with judicial information would be available in the event of a major loss.

95. With appropriate safeguards in place, a court should consider contracting for the use of an alternate “cold site” with a public or private computer recovery service, in order to provide for a physical site to reestablish computer systems and data in the event of a catastrophe or other failure event.

96. For its most sensitive systems, a court could consider contracting for the use of an alternate “hot site” at a public or private computer recovery facility in order to quickly reestablish computer systems and data in the event of a catastrophe or other failure event. The “hot-site” facility would contain compatible hardware and software to that used by the court on a daily basis. When and if a failure event occurs, “hot site” computers can be deployed.

97. If hot or cold site arrangements are not feasible, desktop computer hardware and software can be replaced through emergency purchases immediately following a failure event.

6. Physical Security

Policy 6: All critical network computing equipment should be located in a physically controlled environment, with access limited to personnel responsible for equipment administration and maintenance. The room must be equipped with proper environmental controls. If judicial users have notebook computers, then mechanisms such as laptop locks and alarms should be provided and used to reduce the risk of theft. Disk encryption is strongly encouraged for all notebooks. Controls such as physical access logs and video camera monitoring of network equipment should be implemented. Courts must ensure that when they dispose of any computer device or storage media (including backup tapes) no judicial information can be recovered.

Discussion[16]

98. 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. Some solutions will require the installation of locks, fire extinguishers, surge protectors, window bars, automatic fire equipment, and alarm systems.

99. Courts should ensure that all devices and media used to store judicial information, for example floppy diskettes, recordable CDs and DVDs, hard drives, backup tapes, and solid state storage devices ("USB flash drives"), are either physically destroyed or professionally purged when they are disposed of outside the judiciary. This also includes portable and peripheral devices such as smartphones, PDAs, Blackberries, some printers, digital copiers, multi-function devices, and scanners. Simply deleting files or reformatting the hard drive is not sufficient to remove all traces of potentially confidential data.

100. Secured rooms should have the following features:

- Full-height walls and fireproof walls and ceilings.
- No more than two doors. Doors must be solid, fireproof, lockable, and observable by computing or other staffers.

---

[16] See Wood, paras. 7, ISO 17799, section 9.

- Few and relatively small windows, all of which should have adequate locks.

- Good key control—locking doors and windows are an effective security strategy when appropriate authorities properly maintain keys (card-keys or hard keys or a combination of both types).

- Locally-stored media such as backup tapes should be kept in fireproof and tamper-proof containers.

- Fire extinguishers should be kept near equipment and users should be trained in their proper use. The placement and recharge of fire extinguishers should be checked on an annual basis.

- An uninterruptible power supply ("UPS") should be used to protect critical computing equipment in the event of power outage. Line filters and surge protectors should be installed to control voltage spikes. If recommended in the TRA, some sites might require an alternate power supply unit.

- If judicial users have notebook computers, then mechanisms such as laptop locks and alarms should be provided and used to reduce the risk of theft. Disk encryption is strongly encouraged for all notebooks. Users should be instructed not to leave laptop computers unattended or unsecured while in the office or while traveling to other locations.

- All portable equipment or media containing judicial information should be securely stored behind locked doors.

- Equipment should be labeled in an obvious, permanent, and easily identifiable way, or, if recommended in the TRA, in a covert way. Regular audits should be performed to ensure equipment is in its place.

- When a judicial user has no further need to access judicial information, all keys must be collected, access cards returned and deactivated, and access codes changed. All user access codes should be changed on a periodic basis in any case (at least annually).

7. Classification of Judicial Information

Policy 7: Courts should adopt a classification scheme so that sensitive judicial information may be designated for special protection. Classified information must only be disclosed to those who have a need to know it.[17]

Discussion

101. Courts should establish a classification scheme for judicial information. Classified documents are subject to special handling throughout their life cycle to ensure that only users with appropriate clearance can have access.[18]

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

103. Access to classified information is controlled through the system's management, operational and technical access control systems (see Policy 8). Only those individuals with a legitimate "need to know" should be granted access to read or change (as the case may be) classified information. The author determines who has the need to know.

Classification

104. The following two-level classification scheme provides one very simple model that could be used in a court. Another approach could be to adopt existing classification schemes from the federal or provincial government.

> ***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

---

[17] An information classification scheme is only effective if linked with a court's personnel screening procedure, which is designed to ensure that individuals with access to classified information are trustworthy. Wood, at section 6, "Personnel". provides a variety of policies dealing with human resource matters.

[18] In the course of their work judges already handle information that may be subject to special treatment, such as publication bans, or statutory prohibitions. The Blueprint does not propose to override other security classification schemes that may apply in the judicial context. See also Wood, 5.02 and ISO 17799, section 7.2.

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

105. 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.

Metadata

106. Judges should be aware that some computer files - for example draft judgments – may contain deleted text, revision histories, and embedded personal information that is hidden but readily available to a reader. This embedded text is called "metadata." To ensure that recipients of electronic files, for example by way of e-mail attachment, do not inadvertently gain access to sensitive information of any kind, judicial users should ensure that all computer files leaving the court's secure environment are effectively cleansed of metadata. This cleansing should be handled as an administrative function by the application of appropriate software tools. Software and procedures used for the cleansing process should be audited and validated by the Judicial IT Security Officer.

Implementation

107. Some of the key success factors for a classification scheme are as follows:

- All users must be aware of the classification scheme
- If any system, compilation (database) or storage medium contains classified information, then the entire system, compilation (database) or medium must be so classified
- Classification applies to information from the time it is received or created to the time it is destroyed or declassified
- All classified information must be marked or labeled with the appropriate designation. For example, electronic documents must have a watermark, header or footer appearing on every page. E-mails may have a "signature" designating the level of classification. The systems used should be consistent and typically applied by use of a template
- When classified electronic information is stored on disks or tapes, or printed out in hard copy or faxed from the computer, all media must be

labeled appropriately and the classification designation must appear plainly on all hard copies, title pages and cover sheets

- Classified information must not be printed out at an unattended printer
- If classified information is stored on removable media or on portable equipment, it must be personally attended or locked up at all times
- If backup tapes are stored offsite, classified information must be backed up in encrypted format (See also Policy 5)

108. There are many other specific controls on classified information that courts should consider implementing. A good example of a Data Classification Policy is found at Wood, policy 5.02.01.

Section Three: Technical Safeguards

109. Modern systems management includes the ability to design and configure networks, hardware and software in such a way as to support ITS policies and to enhance (and even automate) operational safeguards. In this section the Blueprint covers System Access Controls, Remote Access Control, Encryption, Firewalls, Intrusion Detection Systems, and Virus Protection.

8. Controlling Access to Court Systems

Policy 8: Courts must implement robust system access controls to ensure that only authorized users have access to any court system, and that their level of access corresponds to their security clearance and the court's information classification scheme. Access rights to classified judicial information must be determined by the judiciary.

Discussion

110. Individuals who are permitted access to court systems should be authenticated by the system. (See Wood, section 9.0, for a detailed collection of policies relating to access control. See also ISO 17799, section 11, "Access Control.")

111. A simple combination of unique username (or "login ID") and password offers a certain minimum level of security. Passwords are vulnerable to being shared, stolen, guessed or calculated. Stronger methods of authentication involve a combination of approaches and more elaborate technologies such as dynamic passwords, smart cards, USB tokens, digital certificates and biometrics.

112. Logical access to judicial information should be logged and routinely audited by the Judicial IT Security Officer. Access to judicial information should be through named individuals only and generic administrative accounts should be avoided. Individuals who do have administrative privileges should have administrative accounts separate from their personal user accounts.

113. Dynamic passwords, which are generated by small portable devices such as tokens, change a user's password every time they log in. Without a token-generated password, logging in is very difficult if not impossible. Used in combination with a static password, these devices prevent anyone from guessing or stealing someone's password.

114. Other devices such as smart cards use digital certificates, which is a form of encrypted user identification. Biometrics use physical characteristics of the user such as a fingerprint or retinal scan. All access control measures add a level of inconvenience to users. Courts must be diligent in encouraging all users not to circumvent or defeat these measures.

115. A court should establish security clearance protocols so that when users log in and are authenticated, their access rights are limited to a level appropriate to their job function. For example, system administrators typically have more rights than users. Typical rights include access to certain servers, folders, applications, features or functionality. (Many of the issues that need to be considered here are covered in chapter 10 of the CSE Handbook.)

Access to Classified Judicial Information

116. Decisions about access rights to classified judicial information must be made exclusively by the judiciary. Some of the decisions that need to be made include:

- Decisions about access to system applications, features or functionality that may impact classified judicial information
- Decisions about the availability of remote access or access to systems in more than one courthouse
- Decisions about an information classification scheme (see Policy 7)
- Decisions about how and when access is removed and files (and backup tapes) are archived or deleted
- Decisions about how much server disk space is allotted to judges
- Any decision or policy related to the potential monitoring of judicial users

Password Protocols

117. System administrators should ensure that users follow established best practices for their password usage. Some examples are provided in Appendix 4, “Ten Things Judges Can Do Now to Improve the Security of Judicial Data.”

118. The court system should enforce password changes on a regular basis and configure all desktops and notebooks with power-on passwords.

119. Work product and other information of judges sharing enterprise-wide e-mail systems can be put at risk if they are listed as users in a way that does not differentiate them from non-judges. Inadvertently sending messages to the wrong person can be more likely in a system where jwatson@court.ca and jane_watson@court.ca are both users on the same domain, but one is a judge and one is a Crown Attorney.

9. Remote Access Control and Wireless Networks

Policy 9: Special measures must be taken to ensure the security and privacy of all remote access connections and wireless networking.

Discussion[19]

120. Canadian judges are peripatetic and many of them take for granted the ability to remotely access court information systems. In addition to the more general access control issues and security needs discussed in the Access Control Systems section above, controls specifically targeting remote access security and the use of portable devices should be implemented. The point where remote access is allowed into the internal network is where a court will be susceptible to hackers and other uninvited guests who can probe and attack network systems. Since remote access and the use of portable devices pose special risks, courts must implement specific controls related to such capabilities.

121. The risks involved in allowing access to the internal network make it crucial to know exactly who all remote users are, what their needs are, and how to incorporate remote access controls into a security plan. The need for secure remote access ("SRA") is not limited to judicial users.

122. Where users dial in to the court system with a modem on ordinary phone lines, to connect to a modem pool or Remote Access Server ("RAS") at the courthouse, courts should consider the following guidelines:

> **Caller ID** – the remote access server checks the telephone number of an incoming call against an approved list of phone numbers. If the phone numbers match, the users gain access to the network. (This method does not address mobile users).
>
> **Callback security systems** – when a user dials into the network, the answering modem requests caller identification, disconnects the call, verifies the caller's identification against a directory, and then calls back the authorized modem at the number matching the caller's identification; thereby denying access to potential hackers. This technique helps ensure that data communication occurs only between authorized devices. Although callback techniques work well for branches and dial-in from a

[19] Wood provides sample Telecommuting and Mobile Computer Security Policies at section 9.08. See also ISO 17799, section 11.7.

user's home, most callback products are not appropriate for mobile or traveling users since these users' locations often vary daily. Products are now available which accept roving callback numbers, allowing mobile users to call into a remote access server or host computer, enter their user ID and password, and then specify a number where the server or host will call them back.[20] The callback number is then logged, and that information is available later to help track down security breaches.

123. Remote users should be authenticated to ensure that only authorized personnel are allowed access to the court's network.

124. Where users access the court system with a digital high-speed connection provided by a cable or telephone high speed Internet Service Provider ("ISP") judges should be provided with firewall software and encrypted VPN technology.[21]

Wireless Networks

125. Wireless networks, which offer users a high level of convenience and mobility, are less secure than hard wired systems. Courts must ensure that all judicial wireless users inside and outside the courthouse are sufficiently protected against security risks through the use of effective training and the application of personal firewalls among other measures. See Wood, sections 8.05.01, 53-59.

126. Wireless LANs and wireless device connections (such as Bluetooth[22]) must be properly configured, secured and tested, and fully compliant with all aspects of information security policy. For example:

- Since WEP (Wired equivalent privacy) is demonstrably unsafe, the newer WPA2 (also known as IEEE 802.11i) standard should be implemented for all wireless networks[23]

- Do not broadcast SSIDs (Service Set Identifiers)

---

[20] This could present problems at locations such as hotel rooms used by judges on circuit where there is no direct analog phone connection.

[21] "Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted." See Webopedia, http://www.webopedia.com/TERM/V/VPN.html.

[22] For information about Bluetooth security, see http://www.bluetooth.com/Bluetooth/Learn/Security/.

[23] For technical assistance see Dan Thompson, "Implementng a Secure Wireless Network for a Windows Environment," SANS Institute, http://www.sans.org/reading_room/whitepapers/wireless/1619.php.

- Change the default SSID and router passwords
- Disable remote management features

Portable Computing

127. An increasing number of judges are using portable computing devices such as smartphones, PDAs (personal digital assistants), Blackberries, and other handheld devices. All such devices should be configured with appropriate security controls before deployment, and all users must be trained in their effective use.

Voice over IP ("VOIP")

128. Voice over IP is a technology that routes telephone communications over networks such as the Internet rather than the traditional public switched telephone network. Though it can save costs and introduce many convenient features such as desktop messaging integration, it also introduces security issues previously unconnected to telephone use. If implementing VOIP, courts should take special care to ensure the system affords the highest available level of security control. See Wood, sections 8.07.07, 28-31.

10. Judicial Independence

Policy 10: 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 CJC Monitoring Guidelines.

Discussion

129. Modern computer networks are like hallways or communications conduits shared by many people, including residents and visitors. While the network itself may be accessible by users with a variety of security clearance levels, only authorized users are given access to specific secure rooms. With appropriate safeguards in place, judicial users and judicial information can be effectively compartmentalized and secured within a single shared network. (See Wood, section 9.04.06 and ISO 17799, section 11: "Access Control.")

130. Some members of the Council are concerned about the management of security on shared court servers in their jurisdictions. They feel that appropriate administrative safeguards may not be in place to protect judicial information, and that the only way judicial information can be entirely secure is with resort to a completely separate physical network for judicial users.

131. Another concern on the part of the Council relates to the principle of judicial independence. The commingling of judicial and non-judicial information, and the presence of crown attorneys or police users on the same network as judicial users, may be seen as compromising that independence.

132. These concerns are strong enough that some judges will store their work product only on removable disks or on their local hard drive, rather than on the network drives provided by the court.

133. The establishment or use of a separate physical network for judicial users would address the independence issue and provide several other benefits, including:

- easier enforcement of access controls and classification scheme
- consistency with Monitoring Guidelines
- more effective means of segregating backups for judicial information

134. However, there also may be practical and economic impediments to the establishment or use of a separate physical network for judicial users, including:

- technical barriers to judicial users who need access to case management and other court administration systems; limitation on access to knowledge that benefits the justice system as a whole
- significant additional expense in creating, managing and supporting parallel computer networks
- additional inconvenience for judicial users having to access two or more network systems
- small, judge-only networks may be even more susceptible to the risk of a security breach than larger, more sophisticated networks

11. Encryption

Policy 11: Courts must make up-to-date encryption technology readily available to judicial users for the storage and transmission of classified judicial information on networks, desktops and notebooks.

Discussion

135. 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.

136. 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.

137. Judicial information that is classified should be encrypted before it is transmitted over a public network. However, the court's ability to audit internal computer systems may be negatively affected if the use of encryption is not managed properly.

138. 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 Judicial IT Security Officer and provide information about the product functionality.

- The Judicial IT Security Officer should instruct all users in the use of encryption technology and should develop and document procedures for recovering encrypted information. The Judicial IT Security Officer should also monitor all user requests for certificates24.

[24] A digital document commonly used for authentication and secure exchange of information on open networks.

12. Firewalls

Policy 12: All court networks containing judicial information must be protected from outside networks including the Internet with appropriate firewall technology that is effectively administered. All connections from a court's network to external networks must pass through approved firewalls.

Discussion[25]

139. Firewalls are an important component of secure network design.[26] They provide a secure gateway to other networks, and help ensure the confidentiality, integrity and availability of judicial information. Firewalls can be configured to (a) block unwanted network traffic and (b) hide information like system names, network topology, network device types, and internal user ID's from the Internet.

140. Considerable research, planning, and a thorough understanding of the court's business, network, systems architecture and security policies are needed to successfully implement firewall systems. The Blueprint establishes some minimum generic guidelines for the procurement, installation, configuration, and maintenance of a network firewall.

141. Firewalls are not an absolute guarantee of network security, and in fact may create a false sense of security among some users. They only extend a perimeter defence around a network. Once an attacker (who may be an authorized user) gains access to the protected network, all systems are at risk.

142. Firewalls also do not prevent attacks through network "backdoors" like dial-up modem connections, direct leased-line connections, or other network departure points. Only network traffic that actually passes through the firewall will be held to its rules; the firewall cannot enforce a policy against traffic using any other network entry points.[27]

---

[25] Wood provides sample firewall policies in Chapter 20, page 633; and at sections 8.05.01, 21-27. See also sections 31-33.

[26] The SANS Institute provides several useful articles on firewalls at http://rr.sans.org/. .

[27] Other malicious traffic such as Trojan horses and key logging programs should not be overlooked, since no perimeter firewall can block it all.

143. If a court network has a dedicated connection to the Internet, then a stand-alone commercial firewall must be in place to protect the network. It is good practice to ensure that application and file servers do not also function as communications servers.

144. Inbound connections to court systems should pass through an identification and access authorization system.

145. If a court desktop or notebook computer is connected to the Internet via a dial-up or dedicated connection, then a personal firewall should be installed and properly configured on that computer.

146. In general a firewall should have the following characteristics and capabilities:

- A product of an established vendor whose products have been certified by government authorities.[28]
- Certified by a national or international standards organization.
- Supports a "deny all services except those specifically permitted" design policy, even if that is not the policy initially used.
- Supports a custom security policy.
- Accommodates new services and needs if the security policy of the organization changes.
- Contains advanced authentication measures or supports ability to install advanced authentication measures.
- Employs techniques to permit or deny services to specified host systems, as needed.
- Logs access to and through the firewall.
- Uses a flexible, user-friendly IP-filtering language that is easy to program and can filter a wide variety of attributes, including source and destination IP address, protocol type, source and destination TCP/UDP port, and inbound and outbound interface.

---

[28] In Canada, a national list of firewalls and VPNs that have been pre-qualified by CSE is found at: http://www.cse-cst.gc.ca/services/industrial-services/its-pre-qual-prod-list-e.html

- If the firewall requires an operating system, such as UNIX, a secured version of the operating system should be included, along with other security tools, as necessary to ensure firewall host integrity—and all operating system patches should be installed.
- The firewall's strength and correctness must be verifiable. Its design should be simple so that administrators can understand and maintain it. The firewall and any corresponding operating system should be updated with patches and other bug fixes.
- Technical support services should be included.
- Training services should be included.
- System documentation should be included.

13. Intrusion Detection System

Policy 13: Courts must establish 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 Judicial IT Security Officer. When recommended in the TRA, courts should install network and host-based (or integrated) intrusion detection systems for real-time and automatic intrusion notification.

Discussion[29]

147. Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of intrusions. Intrusion is defined as an attempt to compromise the security of a computer or network. Intrusion detection may be accomplished either by manually reviewing system-generated logs and taking appropriate action, or by using intrusion detection system software for automated review, analysis, and response to an intrusion. A mix of both manual and automated approaches is usually appropriate.

148. Intrusion detection system ("IDS") software monitors computer systems and network traffic and analyzes that data for possible hostile attacks originating from outside the court, as well as for system misuse or attacks originating from inside. The main advantage of an intrusion detection system is that it provides a clearer view of server and network activity and issues alerts notifying system administrators of unauthorized or unusual activity.

149. Because intrusion detection involves by its nature the monitoring of systems, all intrusion detection systems used in a court must comply with the Monitoring Guidelines (see Appendix 2), which provide that (a) there must be no content monitoring of judicial users and (b) to the extent monitoring of judicial users is required for security purposes, it should be done by judicial users under the direction of the Judicial IT Security Officer.

150. The judiciary needs to develop clear and detailed guidelines for system administration to reduce the risk of conflict.

---

[29] See Wood, sections 9.07 and 8.05.01, 19-20, 8.01.03, 5-6.

Types of Intrusion Detection Systems

151. Currently two primary types of intrusion detection systems are available: host-based and network-based. Some vendors market either a host-based or network-based type of product; however, the trend is to provide an integrated approach that combines both types of IDS products into a centrally managed product that improves network resistance to intrusions and provides greater flexibility in deployment of the products.

152. Host-Based - With the host-based system, the intrusion detection software resides on a server and monitors the server (and some application) logs for unauthorized access attempts and aberrant behaviour patterns. The Judicial IT Security Officer should draft the host-based rules that trigger the analysis of the audit and event logs. The host-based system can then evaluate those actions, such as user or login activity or user account and/or application activity. The host-based systems analyze audit and event logs to look for aberrant patterns of local or remote users that may indicate unauthorized attempts to access the system(s).

153. Network-Based - The network-based type of IDS resides as a sensor on LAN servers. It filters and analyzes network data transmissions in real-time and compares them against a database of known “attack signatures” or patterns. The attack signatures are known methods that intruders have employed in the past to penetrate a network.

154. The following factors should be considered as part of the selection process for Intrusion Detection Systems:

- The vendor must be well established and its products certified by government
- The system should be certified by a national or international standards organization
- The IDS should be able to work in conjunction with network management activity
- The IDS product must be capable of adapting to the changing security needs of the court
- Subscription and signature updates should be included.
- Documentation, technical support and training services should be included

Administration

155. All system audit logs should be reviewed on a daily basis, in compliance with the Monitoring Guidelines.

156. Users should be trained to report any anomalies in system performance. The Judicial IT Security Officer should oversee the review all trouble reports for signs of intrusive activity.

157. Network-based IDS tools should be checked on a routine basis to ensure they are operating as intended.

158. The Judicial IT Security Officer should stay up-to-date with IDS signature file updates (files used to identify potential intrusions based on network traffic characteristics) and have updates implemented in a timely manner.

159. The Judicial IT Security Officer should establish relationships with incident response organizations and Judicial IT Security Officers in other courts, and share relevant threats, vulnerabilities, and incidents discovered.

14. Protection against malicious code, spam and related threats

Policy 14: All court systems must employ industry-standard software to provide real-time detection and protection against malicious code, spam and related threats.

Policy 15: Such protective systems must be configured wherever possible on firewalls, servers, local workstations, notebooks, portable devices and home computers that contain or access judicial information.

Policy 16: All users must be trained in best practices for reducing the threat of malicious code, spam, and related threats.

Discussion[30]

160. Since the advent of Internet e-mail and widespread use of the World Wide Web, malicious code has become a major security threat. Viruses and worms can be transmitted around the world in a short period of time by attaching infected executable files to e-mail messages. The attachments are usually "Trojan horses" masquerading as something the recipient has requested or would like to see, and often appear to be coming from a known source. Adware and spyware are closely related types of malicious code. They are often embedded in legitimate-looking free software, so that when a user downloads the software the spyware is surreptitiously installed at the same time. Typically, malicious code takes control of target computers, using them to launch further co-ordinated attacks on third party web sites, or gaining access to personal information such as passwords.

161. Spam, or unwanted mass e-mail messaging, is said to represent between 75% and 85% of all e-mail traffic.[31] Although at best spam can be considered a nuisance, it is also being used to trick recipients into divulging personal information through a bit of social engineering called "phishing."[32]

162. The best defence against all malicious code is a combination of management practices and the use of protective software on firewalls, servers, workstations, laptops and portable devices (where applicable). Complete protective software should include: a programmable spam filter; a scanner that tests files and directories

---

30 See Wood, section 8.03.01, ISO 17799 section 10.4.

31 Industry Canada, "The Digital Economy in Canada," http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00170e.html.

32 "Phishing is the impersonation of a trusted person or organization in order to steal a person's personal information, generally for the purpose of 'identity theft.'" *Ibid*.

for the presence of malicious code, a "disinfectant" to remove the code from infected files; real-time protection against spam and malicious code; and a subscription service for automated updates to maintain protection as new threats are discovered.

163. The following factors should be considered as part of the spam filtering and malicious code scanning software selection process:

- The vendor should be well established and its products certified by government authority if possible.[33]
- The system should be certified by a national or international standards organization
- The software employs both a scanning engine to detect known threats and a heuristics engine to help identify macro viruses.
- The vendor should provide automatic updates to the spam/code signature file.
- Many security software companies today market protective software solutions for e-mail servers and gateways. It is becoming increasingly important that these two points of entry to the court network be protected. These products must be able to detect and clean infected files (both standard and compressed files) in real-time.
- Capability to be managed and monitored from a central console.
- Policy management capability as part of the software. Important functions that these policy management applications perform include ensuring that end-users cannot circumvent security guidelines, using the court's security policy as a means to deal with malicious code intrusions, and ensuring the Judicial IT Security Officer is notified when security breaches occur.

---

[33] *Blueprint* readers are encouraged to create a short list of vendors by doing their own research or retaining the services of a security expert.

Prevention

164. Users must be made aware of the risks of spam, malicious code and related threats, and trained on the best methods of prevention. This is particularly important for users who access judicial information on home computers.

165. The Judicial IT Security Officer must oversee the approval process for new software applications before they can be installed on a computer. No unauthorized applications may be installed on a computer. Judges must be involved in establishing and reviewing a list of authorized applications. Subject to the Monitoring Guidelines (Appendix 2), software configurations should be scanned on a monthly basis to verify that no extraneous or unknown software has been added to a computer.

166. Software should be downloaded and installed only by or with the authorization of network administrators (who will scan or test software).

167. Protective software should be installed on file servers to limit the spread of malicious code within the network. Workstations should have memory resident software installed and configured to scan data as it enters the computer. All incoming electronic mail should be scanned. Programs and files opened by applications prone to macro viruses should not be executed without prior scanning.

168. It is critical that protective software update files from the vendor be automatically delivered and installed using secure channels.

169. Staff security training should include the following information about the risks of malicious code and spam:

- Protective software is limited to the detection of spam and code that has been previously identified. New and more sophisticated threats are constantly being developed. Scanning software will be updated continuously with new definition files to maintain currency regarding the latest threats.

- All incoming mail and files received from outside the court must be scanned for malicious code as they are received, subject to the Monitoring Guidelines. All checking will be performed if applicable at firewalls that control access to networks. This will allow centralized scanning for the entire organization, and reduce overhead by simultaneously scanning incoming messages that have multiple destinations.

Detection and Security Response

170. Subject to the Monitoring Guidelines, all scanning logs should be recorded, reported and examined by the system administration staff. Users must inform the Judicial IT Security Officer and system administrators of any malicious code that is detected, as well as any configuration change or different behavior of computer systems or applications.

171. Steps should be taken to protect the privacy of any sensitive incoming or outgoing e-mail message or file caught by a spam filter and forwarded automatically to an administrator.

172. When informed that malicious code has been detected, the system administrators should inform the Judicial IT Security Officer and all users who may have access to the same programs or data that their system may be compromised. The users should be informed of the steps necessary to determine if their system is compromised as well as the steps taken to remove the threat. Users should report the results of system scanning and removal activity to the Judicial IT Security Officer and system administrators.

173. All new software must be installed on a test-bed and tested for malicious code before being allowed on an operational machine.

174. To keep abreast of the latest malicious code which has been identified, scanning software should be updated in real time as updates arrive.

175. Any machine infected by malicious code must immediately be disconnected from all networks. The machine should not be reconnected to the network until system administration staff can verify that the threat has been removed.

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.

7. As part of the blueprint, that the following urgent issues be addressed immediately:

   (a) That the Canadian Judicial Council ask the Judges Technology Advisory Committee to create a protocol that addresses security issues related to the use of notebook computers in court-related travel.

   (b) That the Canadian Judicial Council ask the Judges Technology Advisory Committee to co-ordinate with legal and other publishers to:

      (i) Establish procedures to avoid the release of judgments that contain deleted portions or changes;

      (ii) Adopt a protocol to withdraw judgments that contain previous deletions or have been released accidentally.

8. That the Canadian Judicial Council authorize the Judges Technology Advisory Committee to conduct further study in order to make recommendations (with regard to external monitoring of computer use by the judiciary and staff), and ensure that resources are made available to the Committee for that purpose.

Appendix 2: Canadian Judicial Council Monitoring Guidelines

Recommended by the Judges Technology Advisory Committee, July 2002
Approved by the Canadian Judicial Council, September 2002

[1] As a general definition, computer monitoring involves the use of software to track computer activities. Monitoring may include tracking of network activities and security threats, as well as Internet usage, data entry, e-mail and other computer use by individual users. Monitoring is done by someone other than the user, and may be made known to the user or may be surreptitious. In either case, the user has no control over the monitoring activities and the data that is generated.

[2] The effective protection of computer networks against security threats requires certain monitoring activities. However, some types of computer monitoring may represent a significant threat to judicial independence and may also constitute an unlawful invasion of privacy. These guidelines are provided to help judges and system administrators develop appropriate monitoring practices.

[3] As an overriding principle, any computer monitoring of judges, and judicial users 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.

[4] Content-based monitoring of judicial users is not permissible under any circumstances. Prohibited activities include keystroke monitoring, monitoring e-mail, word processing documents or other computer files, and tracking legal research, Internet sites accessed, and files downloaded by individual users.

[5] In order to safeguard the integrity of shared network resources and protect computer systems against hackers and other security threats, procedures may be implemented for monitoring network traffic, logging errors and exceptions, and performing industry-standard maintenance.

[6] Any system integrity and security monitoring must:

Be performed only for legitimate network performance or security management purposes;

Be the least intrusive approach reasonably available. For example, if network resources are affected by a particular activity, system administrators should try to obtain voluntary compliance by educating judicial users about specific information technology concerns.

Gather aggregate information only. Monitoring computer activity and usage patterns by individual judicial users is not permissible, except to ensure that users are validly logged in.

[7] Monitoring data must be kept confidential. Access must be restricted to information technology personnel who need the information to address system integrity and security issues. Electronic monitoring logs and other records must be purged on a regular basis. Statistical information compiled from monitoring data may be retained, provided it contains aggregate information and addresses system integrity and security issues only.

[8] No monitoring may be implemented without the consent of the court's chief justice. Judges must play an integral role in the development and administration of monitoring practices that comply with these guidelines. Any monitoring should be administered by personnel who report directly and are answerable only to the court's chief justice.

[9] Judicial users must be informed of monitoring practices through clear, obvious and consistent notices. Courts should develop acceptable use policies that are communicated when access to computers is first provided. Log-in screens should provide regular reminders about the current policies and the reasons for them.

Appendix 3: Model Protocol for Court Technology Committees (2004)

See http://www.cjc-ccm.gc.ca/cmslib/general/Protocol_CourtTech.pdf

Appendix 4: Ten Things Judges Can Do Now to Improve the Security of Judicial Data

Originally prepared by the Security Subcommittee of the Judges Technology Advisory Committee of the Canadian Judicial Council, May 15, 2002. Second edition, July 26, 2006.

---

1. **Portable devices.** Keep all portable devices such as laptops, Blackberries, PDAs and removable media such as USB flash drives with you when traveling. Otherwise, keep these items securely locked with a safety cable, in a desk drawer, hotel room safe, or in the trunk of your car.
2. **Passwords.** For any computer account, choose a strong password, for example, at least six characters, not a dictionary word or proper noun, combining upper and lower case letters, numbers and symbols. (For example, “FtLYd%7”.) Change your passwords frequently and never share them with anyone. To keep track of all these passwords, use password management software that keeps your passwords readily accessible but encrypted. Never write your passwords down where they can be seen by others.
3. **Backup**. Always make a secure backup of important files if you are not connected to the network. You can use a USB flash drive, an external hard drive, tape device or recordable CD or DVD, as long as you ensure the backup itself is either encrypted, locked up or both.
4. **E-mail**. Never open e-mail attachments from unknown sources, and never click on a link in an e-mail from an unknown or suspicious source, especially if the e-mail is requesting personal information. Such e-mails could be attempts at “phishing,” or dangerous hoaxes masquerading as legitimate messages. Configure and use spam filters to reduce the risk of unwanted intrusions..
5. **Anti-virus and spyware**. Make sure you use available anti-virus and anti-spyware software. Spyware, and its close relative adware, are very persistent examples of malicious software code that take control of web browsers, pop up unwanted ads, and even spy on your computer activities. Always ensure that the protective software signatures are updated on a regular basis, and that the software is set to automatically scan uploaded or downloaded files, websites and e-mail.
6. **Metadata.** Never send computer files (such as draft judgments) outside a secure court environment without making sure that any hidden information such as revisions and deletions from previous drafts, or private personal information (“metadata”) has been cleansed. See “Avoid the Metadata Trap,” forthcoming, *Computer News for Judges*.
7. **Encryption**. Use reliable encryption technology to secure particularly sensitive information stored on your computer whether it is being transmitted or not. You may need to ask your System Administrator for assistance.

8. **Home Operating System**. When prompted periodically by Microsoft Windows to install security patches and fixes to your operating system, confirm the legitimacy of the prompt, and then install the patch to ensure your operating system is current. Prompts from Microsoft are never sent by e-mail. For more information, visit the Microsoft home computing security website: http://www.microsoft.com/athome/security/email/default.mspx
9. **Home wireless networking**. Wireless networks are notoriously weak when it comes to security, but improper installation makes an already poor situation untenable. Make sure you implement all the available security controls on any wireless network. Use the most current equipment to take advantage of recent updates in the wireless security standard.
10. **Monitoring.** Monitoring of judges' computer use raises serious issues about privacy, confidentiality and judicial independence. Chief Justices should identify the appropriate System Administrator and ask for details about the extent to which and ways in which judges' and judicial staff computer use is monitored.

For more information please contact the Canadian Judicial Council by e-mail at info@cjc-ccm.gc.ca or by telephone: (613) 288-1566.

Appendix 5: Glossary of Defined Terms and Acronyms[34]

Term	Meaning
Authentication	Process of verifying an individual's claimed identity
Backup	A routine, regularly scheduled copying of critical system information, configuration and documents to ensure their availability in case the information on servers and workstations is lost.
Bluetooth	A technology that connects devices for short-range data and voice communication without the need for cables.
CA	Certification Authority – a trusted organization that issues digital certificates to individuals for the purpose of authenticating their identity
Certificate	A digital document used to authenticate the sender's identity.
Cryptography	The science of encryption.
CSE	Canadian Communications Security Establishment
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
IT	Information Technology
ITS	Information Technology Security
JCIT	Judicial Committee on Information Technology (Texas)
Judicial staff	Any employees or contractors who report directly to judges and whose work includes the handling of judicial information
Judicial users	Judges and judicial staff
JUDICOM	JUDICOM is the acronym for judicial communication. This is an electronic collaborative tool developed by the Office of the Commissioner for Federal Judicial Affairs to connect federally appointed judges in Canada to the information highway.

[34] The Webopedia is an excellent free online dictionary for computer and Internet technology. The Webopedia is available online at http://www.webopedia.com/.

Term	Meaning
LAN	Local Area Network – a system connecting users to shared computing resources within a building.
Phishing	The impersonation of a trusted person or organization in order to steal a person's personal information, generally for the purpose of 'identity theft.'
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.
PKI	Public Key Infrastructure - a system of digital certificates and authorities that verify the validity of each party involved in an Internet transaction
RAS	Remote Access Server
Real time	With respect to anti-virus programs, a distribution system where updates to anti-virus software are made available as they are developed, not on a scheduled basis, which could delay promulgation.
Spam	Electronic junk mail
Spyware	Malicious code that covertly gathers information about a user through the Internet. Often downloaded unknowingly with free software or shareware.
SRA	Secure Remote Access – provisions for users connecting to local area networks from offsite.
SSID	Service set identifier – used on wireless LANs
SSL	Secure Socket Layer – an encryption protocol for sending information privately over the internet.
TRA	Threat and Risk Assessment
Trojan horse	Malicious program masquerading as a benign object
UPS	Uninterruptible Power Supply – a specialized battery pack that can power a server or a computer for a short time without loss of data if main power is lost.
Virus	Malicious program code designed to spread from user to user via a network
VPN	Virtual Private Network – software for communicating privately across public networks.
Wireless LAN	A local area network using radio frequency rather than wires to connect.
Worm	A special type of replicating virus.

Appendix 6: Model Judicial Acceptable Use Policy for Computer Technology

Approved by the Executive Committee of the Canadian Judicial Council
December 5, 2003

1.0 Overview

1. The<federal/provincial> government provides computer technology for the use of judges and judicial employees in the performance of judicial business.

2. This policy sets out guidelines for the use of computer technology that will help protect computer technology from illegal or damaging actions by individuals, either knowingly or unknowingly, ensure optimum performance of computer systems for all judges and judicial employees, and permit limited personal use to enable judges and judicial employees to be more efficient and productive.

3. The overriding goal is to protect the judiciary and the confidentiality of judicial information by maintaining effective security, which involves the participation and support of every judge and judicial employee who deals with information and/or information systems. Inappropriate use of computer technology exposes the judiciary to risks, including virus attacks, compromise of network systems and services, legal issues, potential security breaches and decreased network efficiency.

2.0 Purpose

The purpose of this policy is to outline acceptable use and best practices for computer technology at <Court Name>.

3.0 Scope

This policy applies to judges and to judicial employees. The Chief Justice/Chief Judge may apply this policy to contractors, consultants, temporary and other judicial staff through incorporation by reference in contracts or memoranda of agreement as conditions for use of computer technology for official business. This policy applies to all computer technology owned or leased by the <federal/provincial> government that is supplied to judges and judicial employees.

4.0 Definitions

For the purposes of this policy, the following definitions apply:

Computer technology includes, but is not limited to, laptops, personal computers and related peripheral equipment, software, Internet connectivity, access to the Court's Internet/Intranet/Extranet/VPN services and e-mail. This list is provided to show examples of computer technology intended to be covered by this policy, but is not meant to be comprehensive.

Employee non-work time means time when judicial employees are not otherwise expected to be addressing judicial business, such as off-duty hours before or after a workday, lunch periods or other authorized breaks.

Judicial employees means employees who report directly to judges and includes judicial assistants, secretaries, consultants, articling students and law clerks.

Limited personal use means use of computer technology by judges and judicial employees for purposes other than judicial business, such as professional activities, career development and reasonable, incidental use for personal purposes. It does not extend to modifying computer technology, such as making configuration changes.

Minimal additional expense means use of computer technology that will result in no more than normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples include using a computer printer to print a limited number of pages, infrequently sending e-mail messages, and occasionally using the Internet.

5.0 Policy

5.1 Security and Proprietary Information

1. It is the responsibility of every judge and judicial employee who uses computer technology supplied by the <federal/provincial> government to be familiar with these guidelines and to conduct their activities in accordance with them.

2. Judges and judicial employees should take all necessary steps to prevent unauthorized access to confidential information.

3. Judges and judicial employees should encrypt information in accordance with the Court's confidentiality guidelines. Draft judgments should be encrypted when sent by e-mail to judicial staff or to other judges, unless the judgment is sent within JUDICOM or a secure internal e-mail system.

4. The <federal/provincial> Information Technology department, with the consent of the Chief Justice/Chief Judge, may perform limited monitoring of computer technology, systems and network traffic pursuant to and in accordance with the Monitoring Guidelines approved by the Canadian Judicial Council. In order to safeguard the integrity of shared network resources and protect computer systems against security threats, procedures may be implemented for monitoring network traffic, logging errors and exceptions and performing industry-standard maintenance. However, content-based monitoring is not permitted.

5. Judges and judicial employees are responsible for the security of their passwords and accounts. Passwords should be kept secure and accounts should not be shared. System-level passwords should be changed quarterly; user-level passwords should be changed every six months. Passwords should not be reused for different accounts, nor should they be saved on computers or web browsers. Passwords should be at least six characters long, combine numbers, letters and alphanumeric characters, and not spell real words.

6. All computers, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computer will be unattended.

7. Because information contained on laptop computers is especially vulnerable, laptops should not be left unattended and, whenever possible, should be secured with a power-on password and a cable locking device.

8. All judges and judicial employees should log off at the end of the workday and turn their computers off.

9. All computers used by judges or judicial employees, whether owned by them or by the <federal/provincial> government, that are connected to the Court's Internet/Intranet/Extranet/VPN, should be continually executing approved virus-scanning software with a current virus database.

10. Judges and judicial employees should be cautious when opening e-mail attachments received from unknown senders, as they may contain viruses.

11. Key documents and work product should be backed up to a server or other secure and reliable media, in accordance with backup procedures established by the Court.

12. Appropriate procedures should be followed to ensure that judgments and other documents being transmitted outside a secure Court environment are free from any hidden information or metadata, such as revisions and deletions from previous drafts or other private information.

13. When disposing of computers, drives, floppies or other storage media, procedures should be followed that are appropriate for the sensitivity of the stored information. Files should not simply be erased but should be purged before recycling or reusing storage media. In some cases media should be physically destroyed, in accordance with the Court's policies.

5.2 Limited Personal Use

1. Computer technology supplied to carry out judicial business offers many conveniences that may be used for personal needs at minimal or no additional cost to taxpayers. This use may enable judges and judicial employees to be more efficient and productive in their professional and personal lives. It also may assist judges who must travel on circuit as part of their judicial duties. Thus, on balance, the limited personal use of computer technology, as permitted in this policy, is in the best interests of the judiciary.

2. Judicial employees are permitted limited personal use of computer technology if such use does not interfere with judicial business and involves minimal additional expense. The limited personal use of computer technology should only occur during judicial employees' non-work time. This privilege may be revoked or limited at any time by the Chief Justice/Chief Judge.

3. Judges are permitted limited personal use of computer technology if such use does not interfere with judicial business and involves minimal additional expense.

4. In using computer technology for limited personal use, judges and judicial employees must, at all times, avoid giving the impression they are acting in an official capacity. If such limited personal use could potentially be interpreted to represent official business of the judiciary, an adequate disclaimer must be used, such as: "The contents of this message are personal and do not reflect any position of the judiciary or the Court."

5. Postings by judges or judicial employees from a Court e-mail address to private newsgroups should contain a disclaimer stating that the opinions expressed are strictly the author's and not necessarily those of the Court, unless the posting is in the course of judicial business. Users should refrain from using Court e-mail addresses for personal postings on public newsgroups or messaging boards, as such postings increase the chances of targeting for marketing or malicious purposes.

5.3. Unacceptable Use

Unacceptable use of computer technology includes:

5.3.1. Deliberate Acts to Circumvent Security

a) circumventing user-authentication or security of any computer, network or account.

b) interfering with or denying service to any user.

c) using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet/VPN.

5.3.2. Performance Issues

a) any personal use that could cause congestion, delay, or disruption of service to any Court or government system, such as downloading large audio or video files.

b) using computer technology in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government.

5.3.3. Illegal and Unethical Activities

a) using computer technology for unlawful activities, which include criminal offences, contraventions of non-criminal regulatory federal and provincial statutes and actions that could make an individual or institution liable to a civil lawsuit.

b) posting judicial information to public news groups, bulletin boards, or other public sites without authority, including any use that could create the perception that the communication was made in an official capacity.

c) creating or transmitting chain letters, e-mail spam or other unauthorized or unsolicited mass mailings, regardless of subject matter.

d) using computer technology in furtherance of a private business.

e) The following activities are also prohibited, except to the extent they are required in the performance of judicial business:

   i) creating, downloading, viewing, storing, copying or transmitting sexually explicit material, material that is inappropriate or offensive to fellow employees or the public, such as hate speech, or material related to illegal gambling and other illegal or prohibited activities.

   ii) providing confidential Court or judicial information, including lists of judges and judicial employees, to parties outside the Court or department of justice.

5.3.4. System Security

a) introducing malicious programs, such as viruses, into networks or servers.

b) revealing an account password to others, except to an authorized user in accordance with Court policy.

c) allowing others, including family and household members, to use an account password or use a computer connected to the Court VPN or Extranet, when work is done at home.

d) attempting to gain unauthorized access to other systems.

5.3.5. Technical Issues

a) effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data that is not intended for the judge or judicial employee or logging into a server or account that the judge or judicial employee is not expressly authorized to access, unless these activities are within the scope of regular duties.

b) port scanning or security scanning, unless prior authorization is given by the Information Technology department.

c) executing any form of network monitoring that will intercept data not intended for the judge or judicial employee.