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.