Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

IT Security and Employee Privacy: Tips and Guidance

June 2015

This guidance document gives an overview of the issues employers should consider before implementing IT security tools that collect employee personal information.

Employees do not check their privacy rights at the office door. There is a right to privacy in the workplace, which has been upheld by Canadian courts and must be respected by public bodies and private sector organizations as they consider what security controls are necessary to protect information in their networks.

INTRODUCTION

Public bodies and private sector organizations are facing an increasing number of internal and external threats to their information technology ("IT") systems. These organizations have an obligation to protect the data stored in their information systems against threats such as malware, social engineering and unauthorized access by employees. Increasingly, they are turning to new and emerging technologies to address and mitigate these threats.

Software solutions can provide some protection, however these tools can also lead to the collection of personal information about employees, through deliberate means (use of employee monitoring software) or inadvertent (network firewalls that monitor website and email traffic).

Employers commonly allow employees to use workplace IT systems for some personal use. Employees are afforded certain privacy rights related to personal use. These privacy rights have been upheld by Canadian courts, privacy commissioners and labour tribunals.

Employees cannot reasonably expect to use employer's computers and other devices in a completely unfettered manner, and employers have a right to ensure employees are not using excessive amounts of work time for personal reasons, like checking social media accounts, or accessing prohibited sites. However, employers must also ensure that an employee's reasonable expectation of privacy is respected in accordance with B.C. laws.

EMPLOYEE PERSONAL INFORMATION

In British Columbia the collection, use, or disclosure of the personal information of employees is governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA") in the public sector and the *Personal Information Protection Act* in the private sector ("PIPA").

Under those laws, "personal information" is generally defined as recorded information about an identifiable individual other than contact information which would enable an individual at a place of business to be contacted. Contact information would include information such as the business telephone number and email address of the individual.

Where, for example, an employee uses their workplace computer during their lunch break to check their online banking or access medical laboratory results, or to communicate with a spouse to plan daycare pickup, personal information could be in play. Any security tool that is monitoring, tracking, or auditing that activity is collecting the personal information of employees.

There are strict legal limits on when public and private sector companies can collect, use or disclose personal information under provincial privacy laws. While there is no one-size-fits-all solution, the following 10 tips will help ensure your IT security system is not running afoul privacy laws through the unauthorized collection of personal information of employees.

TEN WAYS TO PROTECT EMPLOYEE PRIVACY WHEN SECURING THE WORKPLACE

1. Complete a privacy impact assessment

One of the ways for employers to assess privacy risks of any program, policy or software is to complete a privacy impact assessment. This will ensure you have planned out not only how the program will work, but also what type of personal information you will collect and how you can mitigate any potential privacy concerns that result from the program.

Do this work in the early planning stages; don't wait until after you have spent money on a software tool that might put you off-side privacy legislation. Your Privacy Officer can help you complete a privacy impact assessment.

You also have the option of contacting the Office of the Information and Privacy Commissioner for B.C. ("OIPC") and asking us to review your privacy impact assessment. We will provide you with comments, including whether we believe your proposed system is compliant with privacy law. If there are issues, our staff will offer suggestions to help with achieving compliance.

2. Ensure IT and procurement staff consult the privacy officer when considering new security tools and protocols

Violations of privacy can often be unintentional and indirect. When an organization is considering a new security protocol, IT and procurement staff should be in close communication with the organization's privacy officer or legal counsel before decisions are made about implementation, as well as throughout the implementation process.

There are common solutions that address privacy and system security, but an employer needs to ensure that both interests are fully considered at all times in the process.

3. Select IT security tools carefully

Don't assume that a software solution off the shelf using default controls will comply with privacy law. All programs and technologies used must meet the legal threshold for collection of personal information in order to be considered lawful.

In the public sector you must establish that the collection of personal information is **necessary**. This is a high threshold, and you should stand ready to demonstrate what specific purposes you use the security software for, and how it is necessary to your operations as described in s. 26 of FIPPA.

In the private sector the threshold for collection of personal information is what is **reasonable in the circumstances**. Be prepared to explain how your use of security tools – and the personal information they collect – is reasonable for the purposes of establishing, managing or terminating an employment relationship as required by PIPA.

4. Provide notice to employees

Employees are entitled to know what information employers are collecting about them when they use workplace computers, networks, and work-issued smart devices. This information is typically provided for in an employer's Terms of Use policies that are signed by employees upon starting a new job.

Employers should draft these notices carefully. They must state the purpose of the program, the statutory authority for the collection of personal information that results from their IT security protocols, and give the contact information of someone to whom employees can ask questions. Employers should also be prepared to explain to employees how the technology works, the extent of the personal information they will collect and what will be done with that information.

5. Do not engage in continuous, real-time collection of personal information about employees

Employers should be aware that ongoing or real-time collection of personal information from employees, such as keystroke logging and screen capturing, should be restricted to targeted investigations where there are reasonable grounds for suspicion or wrongdoing, and then only when other less privacy-intrusive measures have been exhausted.

Ongoing, continuous and routine monitoring of employee behaviour will seldom be authorized by privacy legislation in other circumstances.

6. Do not collect more personal information than is needed

When assessing possible security solutions, consider the type, volume, and sensitivity of personal information the software might collect and whether it collects more information than you need. Collecting more personal information than is needed for a legitimate business purpose will put you offside privacy law.

Excess collection also creates an unnecessary security risk; employers have a legal responsibility to protect personal information in their custody or under their control.

7. Have policies in place and train your staff

Employers must ensure there are clear, written policies about how the security programs will be operated and secured. These policies include access controls for system data, how long data will be retained, and response plans should a privacy breach occur. Employers must also ensure IT staff have appropriate training on their legal obligations to protect personal information captured by the system.

8. Implement audit logs

Audit logs should keep a record of everyone who accesses the back-end of the IT security system, including network and IT administrators. The audit logs should track when the system was accessed, what data was accessed and whether any changes were made. Employers should review the audit logs periodically to ensure that access is legitimate.

9. Evaluate the effectiveness of IT security programs on an ongoing basis

Is your IT security solution addressing the problem(s) you identified at the outset? Would a less intrusive way of addressing the problem be just as effective? Such an evaluation should take place on an annual basis, at a minimum.

10. When in doubt, ask the OIPC

Our office welcomes questions about any type of IT security organizations are considering. We can help identify compliance challenges and discuss potential solutions to problems.

CONCLUSION: ESTABLISH A CULTURE OF PRIVACY

Good privacy practice is not just about being able to justify your policies or programs should they become the subject of a complaint or investigation by the Information and Privacy Commissioner.

Instead, employers should be working towards ensuring their employees feel they work in an office where their privacy is truly respected and where they are informed of the employer's practices. Such practices will help employers avoid being the subject of a complaint or a privacy investigation.

Our office welcomes employers to ask us questions about any type of IT security they are considering. We can help identify compliance challenges and discuss potential solutions to problems. Employees can also contact us with questions or concerns about privacy rights in the workplace.

If you have any questions about these guidelines, please contact our office by email at INFO@OIPC.BC.CA or by telephone at (250) 387-5629 (in Vancouver call (604) 660-2421; elsewhere in BC call toll free at 1-800-663-7867). For more information regarding the Office of the Information and Privacy Commissioner, please visit WWW.OIPC.BC.CA.

FURTHER READING

Many of the issues discussed in this guidance document have been set out by our office in Investigation Report F15-01, *Use of Employee Monitoring Software by the District of Saanich*, available online at WWW.OIPC.BC.CA/REPORT/INVESTIGATION-REPORTS

These guidelines are for information only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia with respect to any matter within its jurisdiction. These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter, respecting which the Commissioner will keep an open mind.