Implement Personal Data Removal Policy to Prevent Privacy Breaches at Your Company

Don’t let a stolen laptop undermine all of your privacy and cyber security hard work.

Your organization might deploy state-of-the-art IT and cyber security measures to keep personal information confidential. But all it takes is one employee to undo all of your good work by removing the data and getting it lost or stolen. That’s why it’s crucial to implement a policy governing the removal of laptops, iPhones and other personal devices that contain personal information about your customers, clients and employees. Here’s how to create and implement an effective policy.

A Cautionary Tale

A financial planner at a bank decides to take work home with her for the weekend. She downloads files containing private financial information including account numbers and SINs of more than 900 bank customers. She parks her car in the underground garage of her apartment building and leaves the laptop inside on the passenger seat. The car is locked, the alarm armed. The next morning, she finds the passenger side window smashed in and the laptop stolen. Customers are notified that their personal information has been stolen. One of them files a legal complaint against the bank. The Canadian Privacy Commissioner finds the bank guilty of violating the obligation to safeguard personal financial information under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) [*Stolen laptop engages bank’s responsibility*, 2005 CanLII 15488 (PCC)]

The Duty to Safeguard Personal Information

Principle 4.7 of PIPEDA requires that “personal information shall be protected by security safeguards appropriate to the sensitivity of the information.” Privacy laws in AB, BC, NB and other provinces include similar safeguard requirements. Personal information that must be safeguarded includes information not just about a company’s customers but also its employees. The more sensitive the information, the more extensive the safeguards must be. As the case above demonstrates, when one of your employees removes personal information from the office or workplace, it puts your company at risk. If the information gets lost or stolen, you face the prospect of liability under privacy laws, not to mention public embarrassment and damage to your reputation. The rash of incidents involving stolen laptops make this an immediate problem.

But there are also legitimate reasons for employees to take personal information off site, especially in this era of electronic communication and telecommuting and BYOD practices. So, trying to keep all such information within the 4 corners of your workplace is unrealistic and counterproductive. What you need to do is implement as part of your information security policy, a set of ground rules requiring employees who do remove personal information to safeguard it

The Need for an Information Removal Policy

Safeguards required by the law to protect personal information cover the gamut including:

- Electronic measures, such as encryption of data;
- Administrative measures such as limits on which employees can get access to personal information; and
- Physical measures such as keeping data in locked files or areas of the facility.

Restrictions on the removal of data from the company's premises would typically be included as a physical safeguard. Unfortunately, many organizations fail to include such provisions in their information security policies.

How to Create an Information Removal Policy

The privacy laws and guidelines don't specify what to include to safeguard the security of information removed from your workplace. But the Insider spoke to privacy lawyers and consultants about how to draft an appropriate policy. The template policy on the HRI website is based on their recommendations. Like ours, your policy should:

Stress Need to Personal Information Confidential

Principle 4.7.4 of PIPEDA requires organizations to "make their employees aware of the importance of maintaining the confidentiality of personal information." The provincial laws include similar requirements [Policy, Sec. 1].

Describe Purpose of Policy

Explain that the purpose of the policy is to safeguard the removal of personal information by employees from the physical premises of your company [Policy, Sec. 2].

Define Information Policy Covers

It's important to let your employees know exactly what kind of information you're talking about. Indicate that the policy covers personal information regarding customers, employees and other individuals whether in paper or electronic form [Policy, Sec. 3].

Require Prior Approval for Removal of Data

Now comes the heart of the policy—the safeguards themselves. The first safeguard is to establish a procedure requiring employees to notify and secure permission to remove personal information. Designate some person or position at your company to review these requests and exercise discretion about whether to grant them. Our policy names the supervisor but you can change that. The important thing is making sure that the employee furnishes the person reviewing the request enough information to determine:

- Which data the employee proposes to remove;
- What the employee proposes to do with the information;
- How the employee proposes to protect it; and
- When the employee plans to bring it back.

[Policy, Sec. 4].

Require Safeguards Once Data Removal Is Approved

Stipulate the safeguards that employees must use when removing personal information from the workplace, including the completion of a log-out document [Policy, Sec. 5].

Make Infractions Grounds for Discipline

Last but not least, say that employees who violate the policy will be subject to discipline up to and including termination. And follow through if you do discover violations. This might sound like an obvious point, but it was what got the bank in trouble in the PIPEDA case described above. The bank had policies and procedures regarding the safe storage of laptops. But they were just recommendations. The financial planner chose to disregard them, and the bank was found in violation of Principle 4.7 [Policy, Sec. 6].