



## Office of the Information and Privacy Commissioner for Nova Scotia

### 5 Minute Privacy Checkup

As an employee of a public body, municipality or health custodian, you should be aware of your responsibilities to keep personal & sensitive information secure. Current privacy standards require that public bodies, municipalities and health custodians protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This 5-minute privacy checkup asks a series of questions relating to the security of personal information and sensitive business information both hard copy and electronic. A “no” answer to any of these questions is a warning sign that the information may not be secure.

<b>Physical Security</b>		
	Y	N
Do you have files containing sensitive information stored in your office? <ul style="list-style-type: none"><li>• If yes, is the sensitive information stored in a locked filing cabinet?</li><li>• Do you lock your office door whenever you leave the office?</li></ul>		
At the end of the day do you always: <ul style="list-style-type: none"><li>• Clear your desktop of all files containing sensitive information?</li><li>• Store your laptop and all files in a locked filing cabinet?</li><li>• Lock your office door?</li><li>• Log off your computer?</li><li>• Remove all documents containing sensitive information from faxes and printers?</li></ul>		
<b>Email &amp; Faxing</b>		
Before emailing sensitive information do you: <ul style="list-style-type: none"><li>• Ensure that either the owner of the sensitive information has consented to transmission via email or that the information is encrypted?</li><li>• Always attach a confidentiality notice?</li></ul>		
Before faxing any sensitive information do you: <ul style="list-style-type: none"><li>• Only send from a secure fax machine?</li><li>• Prior to sending, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number?</li><li>• Always use a cover sheet that includes both the sender’s name and phone number and the intended recipient’s name and phone number?</li><li>• Always attach a confidentiality notice?</li></ul>		

<b>Security of Electronic Files</b>		
	Y	N
Do you always have to login to any system using a unique identifier and password?		
Is your password complex (numbers, symbols, letters etc) and at least 12 characters?		
Have you changed your password in the last 90 days?		
Do you store all electronic files containing sensitive information on a secure central server? (i.e. no sensitive information stored on local hard drive)		
Is your office computer screen positioned so that no unauthorized individuals can view sensitive information displayed?		
Is your screen saver set to automatically log out after 5 minutes of inactivity?		
<b>Training &amp; Knowledge</b>		
In the last 12 months, have you completed training on privacy and security of sensitive information?		
Do you know whether or not you have authority to collect, use or disclose personal information?		
If you do have authority to collect, use or disclose personal information, do you know the limits and conditions of that authority?		
<b>Mobile &amp; Portable Devices</b>		
Do you always store mobile or portable storage device such as laptops in a locked cabinet when not in use?		
Is all sensitive information contained on your portable storage devices limited to the absolute minimum necessary?		
Have you ensured that all sensitive information contained on any portable storage device you use is encrypted?		
Do you permanently delete sensitive information from your portable storage devices as soon as possible after use?		
<b>Secure Disposal of Sensitive Information</b>		
Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?		
<b>Privacy Habits</b>		
Do you avoid discussing personal information in any area where the conversation can be overheard by unauthorized personnel?		
Do you disclose personal information to co-workers only where the information is necessary for the performance of the duties of your co-workers?		
If you must travel with personal information, do you always ensure that any personal information you have is stored in a locked cabinet or cupboard and never in your car?		

Please see our Reasonable Security Checklist, for more detailed information:  
<https://oipc.novascotia.ca/node/471>

We encourage you to contact us if you have any questions about privacy and security in Nova Scotia.

**Phone: 902-424-4684**  
**Toll Free (NS): 1-866-243-1564**  
**TDD/TTY: 1-800-855-0511**  
**Fax: 902-424-8303**  
**Email: [oipcns@novascotia.ca](mailto:oipcns@novascotia.ca)**