Office of the Information and Privacy Commissioner for Nova Scotia

Reasonable Security Checklist for Personal Information

This checklist was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia[1]. Under Nova Scotia's privacy legislation, public bodies, municipalities and health custodians must all ensure that they have made reasonable security arrangements against such risks as unauthorized access to or use, disclosure, copying or modifications of personal information.[2] This checklist is intended to give a quick snap shot of some key security standards. Failure to meet the standards set out in this checklist is an indication that personal information may be at risk and that a thorough review of security should be undertaken immediately.

The checklist includes questions in each of the 17 areas of security compliance listed below and should take about 30 minutes to complete:

1. Risk Management
2. Policies
3. Records Management
4. Human Resources Security
5. Physical Security
6. Systems Security
7. Network Security
8. Wireless
9. Database Security
10. Operating systems
11. Email and Fax Security
12. Data Integrity and Protection
13. Access Control
14. Information Systems Acquisition, Development and Maintenance
15. Incident Management
16. Business Continuity Planning
17. Compliance

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, *the Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*. This document is based on "Securing Personal Information: A Self-Assessment Tool for Organizations" created by the Office of the Information and Privacy Commissioners in Alberta and British Columbia and the Office of the Privacy Commissioner of Canada. The full self-assessment tool is available at: https://www.oipc.bc.ca/guidance-documents/1439 and as an interactive tool at: https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

[2] *Personal Health Information Act* s. 62, *Freedom of Information and Protection of Privacy Act* s. 24(3), *Municipal Government Act* s. 483(3)

Risk Management		
	Yes	No
1. We have identified all of our personal information assets and their sensitivity.		
2. We have analyzed, evaluated and documented the likelihood of security failures occurring.		
3. We have a risk treatment plan identifying the appropriate management action, resources, responsibilities and priorities for managing personal information security risks.		
Policies		
4. We have operational security policies (such as secure faxing, end-of-day closing, use of couriers).		
5. Employees, contractors and partners have easy access to our personal information security policy.		
6. We have an acceptable use policy.		
Records Management		
7. Specific retention periods have been defined for all personal information.		
8. Personal information contained on obsolete electronic equipment or other assets is securely destroyed before the equipment or asset is disposed of.		
9. Hard copy records containing personal information is shredded, mulched or otherwise securely destroyed.		
Human Resources Security		
10. Training has been implemented for all employees, data custodians and management to ensure they are aware of and understand their security responsibilities, permitted access, use and disclosure of personal information and retention and disposal policies.		
11. All employee are required to sign confidentiality agreements.		
12. Contractors and other third parties are required to return or securely destroy personal information to the public body upon completion of the contract.		
Physical Security		
13. We have strong physical security measures for storing personal information including locked cabinets, pass cards and motion detectors or other intrusion alarm systems.		
14. Our publicly accessible service counters are kept clear of personal information.		
15. We have a nightly closing protocol that requires employees to clear personal information from their desks and lock it away, log out of all computers and remove all documents containing personal information from fax machines and printers.		
System Security		
16. All terminals and personal computers used for handling personal information are positioned so that unauthorized personnel cannot see the screens.		
17. If a user walks away from her terminal there is an automatic process to lock out all users after a short defined period of inactivity.		
18. Personal information is always stored either on a secure server or is encrypted when stored on mobile and portable devices.		

Network Security		
	Yes	No
19. We use perimeter defence safeguards including firewalls, routers, intrusion detection, anti-virus/anti-spyware/anti-malware software) to mediate all traffic and to protect systems that are accessible from the internet.		
20. All systems exposed to the internet or servers supporting sensitive applications are “hardened” (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication).		
Wireless		
21. We have a policy in place that addresses the use of wireless technology.		
22. We have enabled the strongest available security features of the wireless devices, including encryption and authentication.		
23. A wireless intrusion detection and prevention capability is deployed on our network to detect suspicious behaviour.		
Database Security		
24. Automated and/or manual controls have been implemented to protect against unauthorized disclosure of personal information.		
25. There is a formal approval process in place for handling requests for disclosure of database contents or for database access that includes an evaluation of the privacy impacts and security risks.		
Operating Systems		
26. Our operating systems are kept up-to-date with all patches and fixes.		
27. We use a regular schedule for updating definitions and running scans with anti-virus, anti-spyware, anti-malware and anti-rootkit software.		
28. We regularly check expert websites and vendor software websites for alerts about new vulnerabilities and patches.		
Email and Fax Security		
29. We regularly update our fax and email lists.		
30. All of our faxes include a fax cover sheet with sender contact information and a confidentiality notice.		
31. We do not send emails with sensitive personal information unless the recipient has consented to the use of email, the email service is secure or the email itself is encrypted.		
Data Integrity and Protection		
32. We have a procedure in place to ensure that any removal of personal information from the premises has been properly authorized.		
33. We use automated and/or manual controls to prevent unauthorized copying, transmission or printing of personal information.		
Access Control		
34. We have a role based access control policy.		
35. We have a formal user registration process in place.		
36. Each user of our system is uniquely identified.		
37. We limit access privileges to the least amount of personal information required to carry out job related functions.		
38. Users of our system must first be authenticated by username and unique password that is changed at least every 90 days.		

Information Systems Acquisition, Development and Maintenance		
	Yes	No
39. We always identify security requirements as part of any new system development, acquisition or enhancements.		
40. We have controls in place to prevent or detect unauthorized software.		
Incident Management		
41. We have a privacy incident management policy in place and we have assigned an individual to coordinate our response to any incident.		
Business Continuity Planning		
42. We have a backup process in place to protect essential business information.		
Compliance		
43. We regularly monitor system audit logs that relate to the handling of personal information.		
44. We maintain an up to date software/hardware inventory.		
45. We conduct an regular physical inventory of all portable storage devices (laptops, thumb drives, portable hard drives, cell phones).		