March, 2012

Securing Personal Information: A Self-Assessment Tool for Organizations

Office of the Information and Privacy Commissioner of Alberta

Office of the Information & Privacy Commissioner for British Columbia

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Protecting privacy. Promoting transparency.

Introduction

How well is your organization protecting personal information? The personal information security requirements under the *Personal Information Protection Act (British Columbia), Personal Information Protection Act (Alberta)* and the *Personal Information Protection and Electronic Documents Act [PIPEDA] (Canada)* require organizations to take reasonable steps to safeguard the personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The first step in developing reasonable safeguards is to collect only the personal information that is needed for a particular purpose. If it is not needed, organizations should not collect it. But if they do, they need to take appropriate precautions.

Reasonable safeguards include several layers of security, including, but not limited to:

- risk management,
- security policies,
- human resources security,
- physical security,
- technical security,
- incident management, and
- business continuity planning.

The reasonableness of security arrangements adopted by an organization must be evaluated in light of a number of factors including:

- the sensitivity of the personal information,
- the foreseeable risks,
- the likelihood of damage occurring,
- the medium and format of the record containing the personal information,
- the potential harm that could be caused by an incident, and
- the cost of preventive measures.

Generally accepted or common practices in a particular sector or kind of activity may be relevant to the reasonableness of a security safeguard. However, generally accepted practices and technical standards must be complemented by elementary caution and common sense.

In creating this tool, we reviewed other standards (such as those produced by the ISO) and received feedback from various organizations in Alberta, British Columbia, and Atlantic Canada.

Questions in blue indicate the minimum security requirements for any organization, regardless of its size or the sensitivity of the personal information it holds. The remaining questions help organizations raise their security standards beyond those minimum levels.

The goal is to be able to answer "yes" to each question.

Blue text indicates a minimum security requirement.

Contents

1 Risk Management

1.1	Has the organization identified what personal information assets are being held, and their sensitivity?	◯ YES ◯ NO
1.2	Has the organization analyzed, evaluated and documented: The business impacts that might result from personal information security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the information?	◯ YES ◯ NO
1.3	Has the organization analyzed, evaluated and documented: The personal impacts on customers and employees?	◯ YES ◯ NO
1.4	Has the organization analyzed, evaluated and documented: The likelihood of security failures occurring, considering possible threats and vulnerabilities?	◯ YES ◯ NO
1.5	Has the organization analyzed, evaluated and documented: The estimated levels of residual risks?	◯ YES ◯ NO
1.6	Has the organization analyzed, evaluated and documented: Which risks are acceptable?	◯ YES ◯ NO
1.7	Has management formally approved the risk identification in writing?	◯ YES ◯ NO

Risk Treatment

1.8	Does a risk treatment plan identify the appropriate management action, resources, responsibilities and priorities for managing personal information security risks?	◯ YES ◯ NO

Risk Reviews

Are risk assessments conducted at planned intervals to review the residual risks and the identified acceptable levels of risks, taking into account changes to:

1.9	The organization?	◯YES ◯NO
1.10	Technology?	◯YES ◯NO
1.11	Business objectives and processes?	◯YES ◯NO
1.12	Identified threats?	◯YES ◯NO
1.13	Possible future threats?	◯YES ◯NO
1.14	External events, such as changes to the legal or regulatory environment, contractual obligations and social climate?	◯YES ◯NO
1.15	When the organization identifies changes to risks, is the focus and/or priority placed on the most significantly changed risks and their associated preventive action requirements?	◯YES ◯NO
1.16	Are threat and risk assessments (TRAs) scheduled annually?	◯YES ◯NO
1.17	Is there a process trigger for when a non-scheduled TRA or Privacy Impact Assessment (PIA) is required (e.g. security or privacy incident, new threats)?	◯YES ◯NO

Blue text indicates a minimum security requirement.

2 Policies

2.1	Do operational security policies exist? (For example, policies around secure faxing of personal information, policies and procedures for end-of-day closing, policies for using couriers to send personal information and/or policies for reviewing audit logs.)	◯YES ◯NO
2.2	Have the operational security policies been endorsed by management?	◯YES ◯NO
2.3	Has the responsibility for reviewing and updating the organization's policies, procedures, guidelines and standards been defined and assigned?	◯YES ◯NO
2.4	Is the personal information security policy reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness?	◯YES ◯NO
2.5	Are independent reviews of the security policies carried out on a regular basis to ensure compliance with current legislative standards?	◯YES ◯NO
2.6	Are organizational policies and standards updated as a result of this review?	◯YES ◯NO
2.7	Can the security officer responsible for the policy update the policy and republish it to the organization?	◯YES ◯NO
2.8	Do employees, contractors and partners have easy access to the personal information security policy?	◯YES ◯NO
2.9	Do customers have access to information about the organization's personal information security policy?	◯YES ◯NO
2.10	Do incentives exist for employees, contractors, customers and partners to understand and follow the policy?	◯YES ◯NO
2.11	Does the organization track acceptance and measure awareness of security policies?	◯YES ◯NO
2.12	Is there a policy for hardware maintenance and upgrades?	◯YES ◯NO

2.13 Is there a network security infrastructure policy that includes a copy of a current network diagram? ◯YES ◯NO

2.14 Does the network security policy require that system security documentation be protected from unauthorized access? ◯YES ◯NO

2.15 Is there a policy controlling or prohibiting hardware and software not purchased or supported by the organization and their use on the network? ◯YES ◯NO

2.16 If personal information is collected over the Internet, is there a specific policy to manage this practice? ◯YES ◯NO

2.17 Is there a policy that governs access to personal information and IT assets, networks and systems from outside the organization (e.g. remote working, teleworking)? ◯YES ◯NO

2.18 Is there a policy concerning travelling with personal information? ◯YES ◯NO

2.19 Is there an acceptable use policy? ◯YES ◯NO

2.20 Are there policies and appropriate security controls in place governing electronic mail, instant messaging, social networks, blogs, and so on? ◯YES ◯NO

Blue text indicates a minimum security requirement.

3 Records Management

Information Classification

3.1 Is there an information classification policy? ◯YES ◯NO

3.2 Does the information classification policy clearly outline how personal information is to be handled and protected? ◯YES ◯NO

3.3 Have an appropriate set of procedures for information labelling and handling been developed and implemented to support the information classification scheme adopted by the organization? ◯YES ◯NO

3.4 Are users informed of any applicable privacy legislation and repercussions of improper classification? ◯YES ◯NO

Retention of personal information

3.5 Have specific retention periods been defined for all personal information (and in accordance with various legal, regulatory or business requirements)? ◯YES ◯NO

Destruction of personal information

3.6 Is personal information contained on obsolete electronic equipment or other assets securely destroyed before the equipment or asset is disposed of? For example, are the internal hard drives of faxes and printers properly disposed of when replacing old equipment? ◯YES ◯NO

3.7 Are hard copy records containing personal information shredded, mulched or otherwise securely destroyed? ◯YES ◯NO

3.8 Is personal information on magnetic media destroyed by overwriting, degaussing or using some other approved method? ◯YES ◯NO

3.9 Are the contents of erasable storage media containing personal information obscured using an appropriate technique before the medium is reused? ◯YES ◯NO

4 Human Resources Security

Executive Leadership

4.1 Does management actively support personal information security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of personal information security responsibilities? ◯YES ◯NO

4.2 Is there a management-level employee (and management-level contractor representative, where a contract is in place) identified as responsible for security practices? ◯YES ◯NO

4.3 Is there a functional forum of management representatives from IT and business units to coordinate and implement personal information security controls? ◯YES ◯NO

Training

Has training been implemented for all employees, data custodians and management to ensure they are aware of and understand:

4.4 Their security responsibilities? ◯YES ◯NO

4.5 Security policies and practices? ◯YES ◯NO

4.6 Permitted access, use and disclosure of personal information? ◯YES ◯NO

4.7 Retention and disposal policies? ◯YES ◯NO

4.8 Requirements for password maintenance and proper password security? ◯YES ◯NO

4.9 Is annual privacy and security training a requirement for any handling of personal information? ◯YES ◯NO

4.10 Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training? ◯YES ◯NO

4.11 Are there consequences for compromising keys, passwords and other security policy violations? ◯YES ◯NO

4.12 Is completion of privacy and security training tracked? ◯YES ◯NO

Blue text indicates a minimum security requirement.

Human Resources Security (cont.)

Confidentiality Agreements

4.13 Are employees required to sign confidentiality agreements? ◯YES ◯NO

4.14 Do the agreements clearly define individual responsibilities for security, including the protection of personal information? ◯YES ◯NO

4.15 Is responsibility for security an integral part of an individual's annual performance objectives? ◯YES ◯NO

4.16 Is individual performance with respect to security and confidentiality routinely reviewed (i.e., annually) with the individual by management? ◯YES ◯NO

Hiring and Terminations

4.17 Are potential employees who will have access to personal information adequately and appropriately screened? ◯YES ◯NO

4.18 Is there a process to ensure immediate recovery of keys and pass cards, and the revocation of access privileges and appropriate notification of security personnel when a termination (voluntary or involuntary) occurs? ◯YES ◯NO

Contractors and Third Parties

4.19 Are private sector organizations and individuals who have access to personal information adequately and appropriately screened? ◯YES ◯NO

4.20 Are the necessary security requirements specified in any contractual documentation? ◯YES ◯NO

4.21 Do all contracts that involve personal information contain a privacy protection schedule? ◯YES ◯NO

4.22 Are contractors required to comply with the organization's privacy and security policies or equivalent policies to ensure that contractors are bound by the same legislated privacy standards as the organization? ◯YES ◯NO

4.23 Are security controls in place to govern the activities of contractors, customers and partners who may have access to the organization's systems and data? ◯YES ◯NO

4.24 Does a knowledgeable employee supervise external hardware or software maintenance personnel whenever maintenance is undertaken? ◯YES ◯NO

4.25 Are contractors and other third parties required to return personal information to the contracting organization upon completion of the contract? ◯YES ◯NO

4.26 If not required to return the information, are contractors and other third parties required to securely destroy, using an approved method, the information at the completion of the contract? ◯YES ◯NO

4.27 Are there regular inspections and/or audits (scheduled and unscheduled) of contractors and third parties to ensure compliance with security and privacy standards? ◯YES ◯NO

4.28 Are there contractual provisions in place to control outsourcing of any role involving personal information to sub-contractors? ◯YES ◯NO

Blue text indicates a minimum security requirement.

5 Physical Security

Do physical security measures used for storing personal information include:

5.1 Locked cabinets? ◯YES ◯NO

5.2 Locked office doors? ◯YES ◯NO

5.3 Pass cards? ◯YES ◯NO

5.4 Motion detectors and other intrusion alarm systems? ◯YES ◯NO

Is there a secure area for servers containing personal information ensuring:

5.5 Walls extend from the floor to ceiling? ◯YES ◯NO

5.6 Physical access is restricted to authorized personnel? ◯YES ◯NO

5.7 Accesses to the secure space are logged and routinely reviewed? ◯YES ◯NO

5.8 Visitors are escorted by an authorized individual while in the secure space? ◯YES ◯NO

5.9 Motion detectors and alarms are used? ◯YES ◯NO

5.10 If any personal information is stored on local hard drives, is that equipment bolted to the floor? ◯YES ◯NO

5.11 Are publicly accessible service counters kept clear of personal information? ◯YES ◯NO

Is there a nightly closing protocol requiring employees to:

5.12 Clear all personal information from desks and place files containing personal information in locked filing cabinets? ◯YES ◯NO

5.13 Lock all office doors and cabinets? ◯YES ◯NO

5.14 Log out of all computers? ◯YES ◯NO

5.15 Remove all documents containing personal information from fax machines and printers? ◯YES ◯NO

5.16 Set intrusion alarms (where installed)? ◯YES ◯NO

5.17 Are access points such as delivery and loading areas and other points where unauthorized persons may enter the premises controlled and, if possible, isolated from information processing facilities to avoid unauthorized access? ◯YES ◯NO

6 Systems Security

Terminals and Personal Computers

6.1 Are terminals and personal computers used for handling personal information positioned so that unauthorized personnel cannot see their screens? ◯YES ◯NO

6.2 Are terminals and personal computers used for handling personal information positioned so that they are not readily visible from outside the facility? ◯YES ◯NO

6.3 If a user walks away from his or her terminal, is there an automatic process to lock out all users after a defined period of inactivity (e.g. screensaver requiring the authorized user to log on again)? ◯YES ◯NO

Mobile and Portable Devices

6.4 Is there a policy governing the use of mobile devices and removable media if personal information is stored on them? ◯YES ◯NO

6.5 Is the policy reviewed and updated on a regular basis? ◯YES ◯NO

6.6 Does the policy require that the least amount of personal information be stored on the device? ◯YES ◯NO

6.7 Is personal information encrypted when stored on mobile and portable devices, as well as on removable media? ◯YES ◯NO

6.8 Is personal information deleted from mobile and portable devices as soon as possible? ◯YES ◯NO

6.9 Are there reasonable controls in place to prevent the theft of mobile computing and portable devices when left unattended? ◯YES ◯NO

6.10 Are controls in place to prevent or restrict the connection of personal mobile devices (e.g. iPods) or removable media (e.g. USB drives) to the organization's networks and systems? ◯YES ◯NO

6.11 Where mobile or portable devices are allowed to connect to the organization's networks or systems, are they checked to ensure that appropriate security controls (e.g. firewall, anti-virus software) are installed and correctly configured? ◯YES ◯NO

6.12 Are removable media used to store personal information stored in secure containers when not in use? (e.g. locked in a secure cabinet) ◯YES ◯NO

6.13 Are laptops containing personal information cable-locked to desks when in use or otherwise equipped with an alarm that will sound if an attempt is made to remove the laptop? ◯YES ◯NO

Blue text indicates a minimum security requirement.

Systems Security (cont.)

If equipment such as a laptop computer is removed from the premises on a temporary basis by staff, are control procedures in place to:

6.14 Record the identity of the user? ◯YES ◯NO

6.15 Confirm the authority of the user to access the personal information on the equipment? ◯YES ◯NO

6.16 Record the return of the equipment? ◯YES ◯NO

6.17 Is laptop encryption prevented from being disabled by the user? ◯YES ◯NO

6.18 Are laptops equipped with a tracking device, a remote kill-switch, and/or remote deletion of data? ◯YES ◯NO

6.19 Are laptops configured so that users are prevented from changing security settings or downloading other software onto the laptop? ◯YES ◯NO

7 Network Security

Network security includes the system of computers, routers, cables, switches and wireless access points. It is the entire system of transport and storage technologies.

7.1 Are networks segregated physically and/or logically to separate systems containing personal information from public networks such as the Internet? ◯YES ◯NO

7.2 Where a local area network containing personal information is connected to a public network, does the organization use perimeter defence safeguards (e.g. firewalls, routers, intrusion detection or prevention systems, anti-virus/anti-spyware software, etc.) to mediate all traffic and to protect systems that are accessible from the Internet? ◯YES ◯NO

7.3 Are systems that are exposed to the Internet (e.g. web servers and their software) or servers supporting sensitive applications "hardened" (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication)? ◯YES ◯NO

7.4 Are ports closed or Internet connections disabled on computers where services are not needed? ◯YES ◯NO

7.5 Are these safeguards regularly updated? ◯YES ◯NO

7.6 Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches? ◯YES ◯NO

7.7 Are SSL (Secure Socket Layer) or other secure connection technologies (e.g. virtual private network (VPN)) used when receiving or sending personal information? ◯YES ◯NO

Blue text indicates a minimum security requirement.

8 Wireless

WARNING:. We believe that, at this time, there are significant security risks to any handling of personal information using wireless networks. You should therefore carefully consider whether you should use wireless technology to handle personal information. If you do accept the risks, ensure your wireless technology is as secure as possible.

8.1	Is there a policy in place that addresses the use of wireless technology?	◯YES ◯NO
8.2	Does the organization ensure that wireless networks are not used until they comply with the organization's security policy?	◯YES ◯NO
8.3	Are users on the network aware of the risks associated with wireless technology?	◯YES ◯NO
8.4	Does the organization have a complete and current inventory of all wireless devices?	◯YES ◯NO
8.5	Does the organization perform comprehensive security assessments at regular and random intervals (including identifying, locating and removing unauthorized wireless access points and other devices)?	◯YES ◯NO
8.6	Has the organization completed a site survey to measure and establish the wireless coverage for the organization?	◯YES ◯NO
8.7	Are access points located in such a way as to minimize the risk of unauthorized physical access and manipulation?	◯YES ◯NO
8.8	Are access points located in the interior of the organization's premises instead of near external walls and windows?	◯YES ◯NO
8.9	Are default parameters on wireless devices (e.g. passwords, identification codes) changed?	◯YES ◯NO
8.10	Are the strongest available security features of the wireless devices, including encryption and authentication, enabled?	◯YES ◯NO
8.11	Are additional safeguards (e.g. firewalls, anti-virus, etc.) installed on all wireless devices?	◯YES ◯NO
8.12	Are wireless capabilities (e.g. wireless cards in laptops) disabled (either permanently or when not required)?	◯YES ◯NO
8.13	Are unnecessary services (e.g. file sharing) disabled?	◯YES ◯NO
8.14	Is a wireless intrusion detection and prevention capability deployed on the network to detect suspicious behaviour or unauthorized access and activity?	◯YES ◯NO
8.15	Are audit records of security- and privacy-relevant activities on the wireless network created and reviewed on a regular basis?	◯YES ◯NO

9 Database Security

9.1	Is a data dictionary (table of contents) used to document, standardize and control the naming and use of data?	◯YES ◯NO
9.2	Is access to the data dictionary restricted and monitored?	◯YES ◯NO
9.3	Are database maintenance utilities that bypass controls restricted and monitored?	◯YES ◯NO
9.4	If there is a software failure, is the system capable of automatically recovering the database?	◯YES ◯NO
9.5	Have automated or manual controls been implemented to protect against unauthorized disclosure of personal information?	◯YES ◯NO
9.6	Are methods in place to check and maintain the integrity of the data (e.g. consistency checks, checksums)?	◯YES ◯NO
9.7	Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?	◯YES ◯NO
9.8	Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information?	◯YES ◯NO
9.9	Are default parameters on the database (e.g. accounts, passwords, etc.) changed?	◯YES ◯NO
9.10	Is there a formal approval process in place for handling requests for disclosure of database contents or for database access, and does this process include steps to evaluate privacy impacts and security risks?	◯YES ◯NO

Blue text indicates a minimum security requirement.

10 Operating Systems

An operating system is the core software on the computer that allows the operation of all of the other software. The most common operating systems are Microsoft Windows, Mac OSX, Unix and Linux.

10.1	Are operating systems kept up-to-date with all patches and fixes?	◯YES ◯NO
10.2	Is there a regular schedule for updating definitions and running scans with anti-virus, anti-spyware and anti-rootkit software?	◯YES ◯NO
10.3	Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches?	◯YES ◯NO
10.4	Are all network services (e.g. websites or e-mail servers) running on computers connected to the network documented and authorized?	◯YES ◯NO
10.5	Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information?	◯YES ◯NO
10.6	Is accurate time and date information maintained on computers to track malicious usage or errors appropriately?	◯YES ◯NO

11 E-mail and Fax Security

11.1	An organization should consider whether it is appropriate to transmit personal information by e-mail or fax. If it decides to do so, is a policy in place that addresses the use of fax and e-mail transmission of personal information?	◯YES ◯NO
11.2	Are regularly updated lists of fax numbers, e-mail addresses and other contact information produced and distributed to ensure that employees use current and accurate contact information?	◯YES ◯NO

When faxing personal information, are the following steps taken:

11.3	The receiver is notified in advance of the fax?	◯YES ◯NO
11.4	The receiver stands by to receive the data or the receiver confirms that their fax machine is in a secure location?	◯YES ◯NO
11.5	The sender takes the utmost care to ensure the accuracy of the fax number dialled?	◯YES ◯NO
11.6	A fax cover sheet is always used and always includes the name, address and phone number of both the sender and receiver?	◯YES ◯NO
11.7	The transmission is encrypted?	◯YES ◯NO
11.8	A confidentiality notice is attached?	◯YES ◯NO
11.9	Are pre-programmed fax numbers regularly checked to ensure accuracy?	◯YES ◯NO
11.10	Are fax machines used to send or receive personal information positioned in a secure area?	◯YES ◯NO
11.11	Is access to fax machines used to send and receive personal information controlled using access keys and passwords?	◯YES ◯NO
11.12	Are fax activity history reports retained to check for unauthorized transmissions?	◯YES ◯NO
11.13	Are the internal hard drives of faxes and printers properly disposed of when replacing old equipment?	◯YES ◯NO
11.14	Are fax confirmation reports carefully checked to ensure the correct transmission of personal information?	◯YES ◯NO
11.15	Are fax machines used for the transmission and receipt of personal information only used by authorized staff?	◯YES ◯NO
11.16	When sending e-mail messages to more than one recipient, is the bcc field used?	◯YES ◯NO

Blue text indicates a minimum security requirement.

12 Data Integrity and Protection

This section is intended to be specific to securing the data from unauthorized modification.

12.1 Is there a procedure in place to ensure that any removal of personal information from the premises has been properly authorized? ◯YES ◯NO

12.2 Is there an archiving process that ensures the secure storage of data, and guarantees the continued confidentiality, integrity and availability of the data? ◯YES ◯NO

12.3 Are encryption and other secure mechanisms in place for both the transport and storage of personal information? ◯YES ◯NO

12.4 Are automated or manual controls, or both, used to prevent unauthorized copying, transmission, or printing of personal information? ◯YES ◯NO

12.5 Are there policies and procedures in place to protect against unauthorized modification of data? ◯YES ◯NO

12.6 When transmitting personal information where data integrity is a concern, is an integrity mechanism used to verify that the data has not been altered during transmission (e.g. digital signatures)? ◯YES ◯NO

12.7 Is there a process to revert and resolve changes if the data-integrity verification process fails? ◯YES ◯NO

12.8 Are data and software integrity tools (such as Tripwire) used to detect unexpected changes to files? ◯YES ◯NO

13 Access Control

General

13.1 Is there an access control policy? For example, are there policies requiring username and password when you log in? Are there policies governing access to the operating system and each database? ◯YES ◯NO

13.2 Does the network access policy include a requirement that each user, at login, is informed of the date and time of the last valid logon and any subsequent failed logon attempts? ◯YES ◯NO

13.3 Are controls in place to detect any discrepancies in logon attempts? ◯YES ◯NO

User Registration, Access and Approval

13.4 Is a formal user registration process in place? ◯YES ◯NO

13.5 Does the user registration process include: verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not granted until formally approved? ◯YES ◯NO

13.6 Is each user of a system that processes personal information uniquely identified? ◯YES ◯NO

13.7 When assigning a unique identifier for users, does the organization ensure the proper identification of the individual to whom the identifier is being issued, before giving the user access to the system? ◯YES ◯NO

13.8 Is the identification of the authorizer retained in the transaction record? ◯YES ◯NO

13.9 Is a current, accurate inventory of computer accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts? ◯YES ◯NO

Blue text indicates a minimum security requirement.

Access Control (cont.)

Roles

13.10 Is there a formal process to assign defined roles to users? ◯YES ◯NO

13.11 Does the access control policy clearly state the information access privileges for each defined role in the organization? ◯YES ◯NO

13.12 Does the role assignment process contain steps to ensure personal information is withheld from unauthorized individuals (e.g. manufacturers, maintenance staff)? ◯YES ◯NO

13.13 Is a data custodian role defined that includes access control, data integrity, as well as backup and recovery? ◯YES ◯NO

13.14 Has the role been defined for maintaining the access control lists? ◯YES ◯NO

13.15 Are roles and access rights for partners and third-party organizations (such as consultants, off-site storage) clearly defined? ◯YES ◯NO

13.16 Are privileges allocated on a need-to-use basis, and allocated, modified or changed only after formal authorization? ◯YES ◯NO

13.17 Are access privileges limited to the least amount of personal information required to carry out job-related functions? ◯YES ◯NO

13.18 Is there a clearly defined separation or segregation of duties (e.g. someone who initiates an event cannot authorize it; roles cannot overlap)? ◯YES ◯NO

13.19 Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals? ◯YES ◯NO

Authentication

13.20 Where a system user is authenticated, is the authentication information, such as password, not displayed, and is it protected from unauthorized access? ◯YES ◯NO

Where user identification and authentication mechanisms are used to protect personal information, are procedures implemented that:

13.21 Control the issue, change, cancellation and audit of user identifiers and authentication mechanisms? ◯YES ◯NO

13.22 Ensure that authentication codes or passwords are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code? ◯YES ◯NO

13.23 Are the authentication mechanisms that are implemented commensurate with the sensitivity of the information and the associated risks (i.e. the more sensitive the information, the more robust the authentication mechanisms. For example, is two-factor authentication used when handling sensitive personal information, including financial information)? ◯YES ◯NO

13.24 Where authentication is based on username and password, are effective password policies in place? ◯YES ◯NO

Are passwords:

13.25 Known only to the authorized user of the account? ◯YES ◯NO

13.26 Pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition? ◯YES ◯NO

13.27 No less than eight characters in length? ◯YES ◯NO

13.28 One-way encrypted? ◯YES ◯NO

13.29 Excluded from unprotected, automatic logon processes? ◯YES ◯NO

13.30 Changed at least semi-annually? ◯YES ◯NO

13.31 Changed at frequent and irregular intervals? ◯YES ◯NO

Blue text indicates a minimum security requirement.

14 Information Systems Acquisition, Development and Maintenance

Hardware

14.1 Are security requirements identified as part of any new system development, acquisition or enhancement? ◯YES ◯NO

14.2 Does the organization have a configuration-management or change-control process (e.g. source code control, tickets and resolutions)? ◯YES ◯NO

Software

14.3 Are privacy and security considered in the process of obtaining new third-party software? ◯YES ◯NO

14.4 Is there a patch management process for new security vulnerabilities? ◯YES ◯NO

14.5 Is there a separate environment for development and testing? ◯YES ◯NO

14.6 Do the development and testing environments contain test data only? Test data should not be drawn from current or past real data. ◯YES ◯NO

14.7 Are development personnel restricted from having access to the production environment? ◯YES ◯NO

14.8 Is there a policy that prohibits the use of unauthorized software? ◯YES ◯NO

14.9 Are there controls that prevent or detect unauthorized software? ◯YES ◯NO

Maintenance

14.10 Are systems containing personal information maintained only by appropriately screened personnel? ◯YES ◯NO

15 Incident Management

15.1 Is there a privacy incident management policy in place? Has the organization appointed an individual or established a centre to coordinate incident response? ◯YES ◯NO

15.2 Is there a privacy incident management policy in place? Do these procedures include guidance for the exchange of incident-related information with designated individuals and organizations in a timely fashion? ◯YES ◯NO

Does the privacy incident management policy include:

15.3 Incident detection and analysis ◯YES ◯NO

15.4 Containment, mitigation and recovery strategies ◯YES ◯NO

15.5 Notification and reporting requirements ◯YES ◯NO

15.6 Post-incident analysis ("lessons learned") ◯YES ◯NO

15.7 Prevention strategies ◯YES ◯NO

15.8 Are the individuals assigned to incident response roles adequately trained? ◯YES ◯NO

15.9 Are the incident response procedures practised and tested on a regular basis? ◯YES ◯NO

15.10 Does the organization use a variety of mechanisms (e.g. firewalls, routers, intrusion detection and prevention systems, audit logs, system performance tools, etc.) to continuously monitor the operations of their systems to detect anomalies in service delivery levels? ◯YES ◯NO

Blue text indicates a minimum security requirement.

Incident Management (cont.)

Does the organization maintain records that show how incidents were handled, including:

15.11 Documenting the chain of events during the incident, noting the date and time when the incident was detected? ◯YES ◯NO

15.12 The actions taken? ◯YES ◯NO

15.13 The rationale for decisions made? ◯YES ◯NO

15.14 Details of any communications? ◯YES ◯NO

15.15 Management approvals or direction? ◯YES ◯NO

15.16 Any external and internal reports? ◯YES ◯NO

Does the organization perform a post-incident analysis that summarizes the cause and impact of the incident, including costs, and identifies:

15.17 Security deficiencies? ◯YES ◯NO

15.18 Measures to prevent a similar incident (e.g. modifications to existing safeguards or the addition of new safeguards)? ◯YES ◯NO

15.19 Measures to reduce the impact of a recurrence? ◯YES ◯NO

15.20 Improvements to incident response procedures? ◯YES ◯NO

16 Business Continuity Planning

Organizations need to ensure that they can continue to operate in the event of an interruption to their operations (e.g. IT system failures, supply chain problems, natural disasters).

16.1 Is there a process in place to develop and maintain business continuity throughout the organization? ◯YES ◯NO

16.2 Has the organization conducted an impact analysis to identify and prioritize the organization's critical services and assets? ◯YES ◯NO

Does the business continuity plan address:

16.3 Different levels of interruption of service? ◯YES ◯NO

16.4 Physical damage? ◯YES ◯NO

16.5 Environmental damage? ◯YES ◯NO

16.6 Unauthorized modification or disclosure of information? ◯YES ◯NO

16.7 Loss of control of system integrity? ◯YES ◯NO

16.8 Physical theft? ◯YES ◯NO

16.9 Has the organization made provisions for the continuous review, testing and audit of business continuity plans? ◯YES ◯NO

16.10 Has the business continuity plan been subject to appropriate departmental or regulatory expert review (e.g. legal, policy, finance, communications, information management and human resource specialists)? ◯YES ◯NO

16.11 Are backup processes in place to protect essential business information such as production servers, critical network components, configuration backup, etc? ◯YES ◯NO

16.12 Are backups stored off site? ◯YES ◯NO

16.13 Are remote backups and recovery procedures tested at regular intervals? ◯YES ◯NO

16.14 Where 100% availability is essential, are duplicate databases maintained on separate physical devices and are all transactions performed simultaneously on both databases? ◯YES ◯NO

16.15 Have all databases and data repositories been identified? ◯YES ◯NO

16.16 Are mechanisms in place to monitor the organization's level of overall readiness? ◯YES ◯NO

Blue text indicates a minimum security requirement.

17 Compliance

Audit Process Design

17.1 Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system? ◯YES ◯NO

17.2 Are all system/audit logs that relate to the handling of personal information: Securely and remotely logged to a read-only medium that has an alert system when tampering is attempted? ◯YES ◯NO

17.3 Are all system/audit logs that relate to the handling of personal information: Regularly monitored? ◯YES ◯NO

Ongoing Audits

17.4 Are procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly? ◯YES ◯NO

17.5 Are proactive audits conducted at regular intervals to verify the logical and physical consistency of the data, in order to identify discrepancies such as lost records, open chains, incomplete sets and improper usage? ◯YES ◯NO

17.6 Is active monitoring in place to ensure that personal information cannot be passed between computers, or between discrete systems within the same computer, without authority? ◯YES ◯NO

Scheduled Audits

17.7 Is software/hardware inventory maintained in an up-to-date fashion? ◯YES ◯NO

17.8 Is an annual physical inventory of all storage media containing personal information performed and are discrepancies investigated immediately and corrected? ◯YES ◯NO

Audit Verification

17.9 Are audit monitoring and review procedures in place to promptly detect errors in procedures and results? ◯YES ◯NO

Audit Implementation

17.10 Do the management personnel responsible for the audited area oversee the implementation of audit recommendations, verify completion of implementation and report verification results? ◯YES ◯NO

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4
Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca