SECURITY

October 2020

Securing personal information

A self-assessment tool for public bodies and organizations

Office of the Information and Privacy Commissioner of Alberta

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Table of Contents

Introduction

How well is your organization or public body protecting personal information? The personal information security requirements under British Columbia and Alberta's *Personal Information Protection Acts* and *Freedom of Information and Protection of Privacy Acts* and Canada's *Personal Information Protection and Electronic Documents Act* require organizations and public bodies[1] to take reasonable steps to safeguard the personal information in their custody or control. Risks that you must guard against include unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The first step in developing reasonable safeguards is to limit the collection of personal information to only what is needed for a particular purpose. If the personal information is not needed, organizations should not collect it.

The next step for organizations is to ensure reasonable safeguards are in place to protect the personal information they have collected.

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

- risk management
- written privacy and security policies
- human resources security
- physical security
- technical security
- incident management
- business continuity/disaster recovery planning

The reasonableness of security measures adopted by an organization must be evaluated considering 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
- industry standards

Generally accepted or common practices in a particular sector may be relevant to the reasonableness of a security safeguard. However, you must complement generally accepted

[1]For the purpose of this document, organization is used to include both private sector organizations and public bodies.

practices and technical standards by elementary caution and common sense. In a digital world, it is more important than ever that organizations and public bodies maintain trust by making all reasonable efforts to avoid a breach.

In creating this tool, we reviewed global security standards such as those produced by the International Standards Organization, and consulted with local security experts.

To conduct your security self-assessment, check off each completed task. The goal is to be able to check off each question.

1. Risk management

- ☐ 1.1 Has your organization identified what personal information assets are being held, and their sensitivity?
- ☐ 1.2 Has your organization documented its personal information assets, where they are held, and their sensitivity (for example, in a personal information inventory)?
- ☐ 1.3 Has your organization analyzed, evaluated, and documented the business impacts that might result from personal information security failures, considering the consequences of a loss of confidentiality, integrity or availability of the information?
- ☐ 1.4 Does your organization perform a Privacy Impact Assessment (PIA) that analyzes, evaluates and documents the personal impacts on customers and employees if an information breach were to occur?
- ☐ 1.5 Does your organization have a standard security threat and risk assessment (STRA) method to document information security risk?
- ☐ 1.6 Has your organization analyzed, evaluated and documented the estimated levels of remaining risks to existing and new information systems?
- ☐ 1.7 Has your organization analyzed, evaluated and documented the acceptability of risks to personal information for the project, program, system, or activity?
- ☐ 1.8 Are risk assessments conducted at planned intervals to review the residual risks and the identified acceptable levels of risks?
- ☐ 1.9 Has management formally approved the risk identification and acceptance in writing?

Risk Treatment

- ☐ 1.10 Are risk treatment plans created to address personal information security risks by identifying the appropriate management action, resources, responsibilities and priorities for managing each risk?

2. Policies

☐	2.1	Does your organization have documented operational information security policies?
☐	2.2	Have the security policies been endorsed by management?
☐	2.3	Has the responsibility for reviewing and updating your organization's security policies, standards, procedures and guidelines been defined and assigned?
☐	2.4	Are the information security policies reviewed at planned intervals or when significant changes occur, to ensure its continuing suitability, adequacy, effectiveness, and compliance with current legislative standards?
☐	2.5	Are organizational policies and standards updated because of this review?
☐	2.6	Can the person responsible for the policy update the policy and republish it to the organization once management has approved them?
☐	2.7	Do employees, contractors and partners have easy access to information about security and privacy polices?
☐	2.8	Do customers have access to information about information security and privacy policies?
☐	2.9	Does your organization document whether employees commit to following security policies?
☐	2.10	Is there a policy requiring hardware and software assets to be maintained with the latest critical security patches and upgrades in a reasonable timeframe?
☐	2.11	Is there a network security policy or standard that governs network access and includes use of cloud-based services, partner networks and remote connectivity?
☐	2.12	Does the network security policy require that system security documentation be protected from unauthorized access?
☐	2.13	Is there a policy or standard controlling or prohibiting hardware and software assets not purchased or supported by your organization (for example staff-owned devices, contractor devices)?
☐	2.14	Is there a policy that governs access to personal information and IT assets, networks and systems from outside your organization (for example remote working, teleworking)?
☐	2.15	Is there a policy or security standard concerning travelling with personal information?
☐	2.16	Is there an acceptable use policy for IT assets and personal information?

☐ 2.17 Are there policies and appropriate security controls in place governing all forms of electronic communications (email, messaging, social media, etc.)?

3. Records management

Information classification

☐ 3.1 Is there an information classification policy?

☐ 3.2 Does the information classification policy clearly outline how personal information is to be managed and protected?

☐ 3.3 Have information labelling and handling procedures been developed and implemented to support information classification?

☐ 3.4 Are users informed of any applicable privacy legislation and repercussions of improper classification?

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)?

Destruction of personal information

☐ 3.6 Is personal information contained on electronic equipment or other assets securely destroyed before the equipment or asset is disposed of? For example, are the internal hard drives of faxes, scanners, and printers properly disposed of when replacing old equipment?

☐ 3.7 Are hard copy records containing personal information cross-shredded, mulched or otherwise securely destroyed?

☐ 3.8 Is personal information on magnetic media destroyed by overwriting, degaussing or using some other approved method?

☐ 3.9 Are the contents of erasable storage media containing personal information securely erased or over-written before the media is reused?

4. Human resources security

Executive leadership

☐ 4.1 Does management actively support personal information security within your organization? For example, does management prioritize and fund privacy and security initiatives, demonstrate compliance with policies and champion awareness?

☐ 4.2 Is there a senior management-level employee identified as being responsible for information security practices (for example CIO, CISO, CPO)?

☐ 4.3 Is there a functional forum of management representatives from IT and business units to coordinate and implement personal information security controls?

Training

4.4 Has your organization trained all employees, privacy officers, management, and others who may access personal information collected by your organization to ensure they are aware of and understand their responsibilities regarding:

- ☐ Handling personal information assets?
- ☐ Security policies and practices?
- ☐ Permitted access, use and disclosure of personal information?
- ☐ Retention and disposal policies?
- ☐ Access control and password management?
- ☐ What to do in the event of a breach or other information incident?

☐ 4.5 Is annual privacy and security training a requirement for any employee handling personal information?

☐ 4.6 Is completion of privacy and security training tracked?

☐ 4.7 Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training?

☐ 4.8 Are there consequences for security policy violations such as compromising access credentials (for example passwords, keys, etc.)?

☐ 4.9 Are employees educated about common threats related to social engineering (for example spoofing, phishing, link manipulation, etc.) and what to do if they encounter these threats?

Employee responsibilities

☐ 4.10 Are individual responsibilities for information security clearly defined and communicated to employees?

☐ 4.11 Is individual performance with respect to security and confidentiality reviewed with employees by management at least annually?

Hiring and terminations

- ☐ 4.12 Are potential employees who will have access to personal information subject to security screening / background checks such as reference and criminal records checks?
- ☐ 4.13 Are employees required to sign confidentiality agreements?
- ☐ 4.14 Is there a mandatory termination process to ensure immediate recovery of keys and pass cards, the revocation of access privileges and notification of security personnel?

Contractors and third parties

- ☐ 4.15 Are third-party private sector organizations and individuals who have access to your organization's facilities or personal information subject to the same security screening as employees (for example cleaners, maintenance workers, researchers, students, etc.)?
- ☐ 4.16 Do all contracts contain an information security schedule that includes confidentiality and protection requirements?
- ☐ 4.17 Do all contracts that involve personal information contain a privacy protection schedule?
- ☐ 4.18 Do all contracts contain a requirement to report any suspected breaches or information incidents to your organization?
- ☐ 4.19 Are contractors required to comply with the organization's privacy and security policies or equivalent policies?
- ☐ 4.20 Are security controls in place to govern the activities of contractors, customers and partners who may have access to your organization's systems and data?
- ☐ 4.21 Does a knowledgeable employee supervise external hardware or software maintenance personnel whenever maintenance is undertaken?
- ☐ 4.22 Are contractors and other third parties required to return personal information to the contracting organization upon completion of the contract?
- ☐ 4.23 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?
- ☐ 4.24 Are there regular inspections and/or audits (scheduled and unscheduled) of contractors and third parties to ensure compliance with security and privacy policies and standards?
- ☐ 4.25 Are there contractual provisions in place to control outsourcing of any role involving personal information to sub-contractors?

5. Physical Security

- ☐ 5.1 Is there a physical security policy in place to prevent asset loss?
- ☐ 5.2 Are all facilities containing IT assets protected by sufficient controls to prevent or detect unauthorized entry or removal of assets?
- ☐ 5.3 Are all employees and authorized visitors required to wear visible identification badges?
- ☐ 5.4 Are all employees required to secure any physical devices or files containing personal information in a locked office, desk, cabinet or file room when unattended or not in use?
- ☐ 5.5 Is physical access to servers restricted to authorized personnel?
- ☐ 5.6 Are accesses to the secure space logged and routinely reviewed?
- ☐ 5.7 Are visitors escorted by an authorized individual while in the secure space?
- ☐ 5.8 Are motion detectors and alarms tested frequently to confirm operation?
- ☐ 5.9 Is encryption required on any electronic media (hard disks, soft media, USB drives, etc.) that personal information is stored on?
- ☐ 5.10 Are publicly accessible service counters kept clear of personal information?
- 5.11 Is there a nightly closing protocol requiring employees to:
  - ☐ Clear off and secure all files from desks (for example clean desk policy)?
  - ☐ Log out of all computers?
  - ☐ Remove all documents containing personal information from fax machines and printers?
  - ☐ Set alarms (where installed)?
  - ☐ Lock filing cabinets and individual office doors?

6. Systems security

Workstation computers

- ☐ 6.1 Are terminals/computers used for handling personal information positioned so that unauthorized personnel cannot see their screens?
- ☐ 6.2 Are terminals/computers used for handling personal information positioned so that they are not readily visible from outside the facility?
- ☐ 6.3 Is there an automatic screen lock enabled after a defined period of inactivity?

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?
- ☐ 6.5 Is the policy reviewed, updated and communicated on a regular basis?
- ☐ 6.6 Does the policy require that the least amount of personal information be stored on the device?
- ☐ 6.7 Is personal information encrypted when stored on mobile and portable devices, as well as on removable media?
- ☐ 6.8 Is personal information deleted from mobile and portable devices as soon as possible?
- ☐ 6.9 Are controls in place to prevent the theft of mobile and portable devices when left unattended?
- ☐ 6.10 Are controls in place to prevent or restrict the unauthorized connection of personal mobile devices or removable media (for example USB drives) to your organization's networks and systems?
- ☐ 6.11 Where personal mobile devices are allowed to connect to your organization's network, are they checked to ensure that they meet security policy and standards?
- ☐ 6.12 If personal owned devices are allowed by your organization, do you have measures in place to separate corporate and personal information logically (by properly implementing a mobile device management solution)?
- 6.13 If equipment such as a laptop computer is removed from the premises on a temporary basis by staff, are control procedures in place to:
  - ☐ Record the identity of the user?
  - ☐ Confirm the authority of the user to access the personal information on the equipment?
  - ☐ Record the return of the equipment?
  - ☐ Prevent a user from disabling hard disk encryption?
  - ☐ Allow tracking of the device, remote disabling of the device, or remote deletion of data on the device?
  - ☐ Prevent users from changing security settings or downloading unauthorized software onto the laptop?

7. Network security

An organization's network is comprised of the entire system of technologies used to process, transport and store electronic data, including cloud services. Network security includes all controls used to prevent, detect and respond to unauthorized activity on the network.

- ☐ 7.1 Are there controls in place to prevent, detect, and respond to security incidents?
- ☐ 7.2 At the minimum, are technologies such as firewall, intrusion prevention, web content filtering, email content filtering, and anti-malware implemented?
- ☐ 7.3 Are all systems and devices configured to use available security controls and minimize attack surface by disabling unnecessary services and applications?
- ☐ 7.4 Are internal networks segregated by security transit points that enforce access restrictions, monitor traffic, and prevent unauthorized actions?
- ☐ 7.5 Are these safeguards regularly updated?
- ☐ 7.6 Is there a patch management program to ensure that critical security patches are deployed in a timely manner?
- ☐ 7.7 Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and security patches?
- ☐ 7.8 Is there a vulnerability management program in place to detect vulnerable systems and implement measures to prevent a breach?
- ☐ 7.9 Are secure communication technologies (for example SSL/TLS, virtual private network (VPN)) used when sending or receiving personal information across the network?

8. Wireless

Note: The use of wireless network technology poses significant security risks to any handling of personal information, especially over public 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?
- ☐ 8.2 Does your organization ensure that wireless networks are not used until they comply with the organization's security policy?
- ☐ 8.3 Are the strongest available security features of the wireless devices, including encryption and authentication, enabled?

- ☐ 8.4 Are staff educated on the risks associated with wireless technology?
- ☐ 8.5 Does your organization have a complete and current inventory of all wireless access point devices?
- ☐ 8.6 Does your organization conduct periodic security assessments to identify, locate and remove unauthorized or non-compliant wireless access points and other devices?
- ☐ 8.7 Does your organization conduct site surveys to establish coverage exposures outside the organizational facility?
- ☐ 8.8 Are access points located in such a way as to minimize the risk of unauthorized physical access and manipulation?
- ☐ 8.9 Are default parameters on wireless devices (for example passwords, identification codes) changed frequently?
- ☐ 8.10 Are safeguards (for example firewalls, intrusion prevention, etc.) deployed on your organization's wireless networks to detect and prevent unauthorized activity?
- ☐ 8.11 Are audit records of security- and privacy-relevant activities on the wireless network created and reviewed on a regular basis?

9. Database security

- ☐ 9.1 Is a data dictionary (table of contents) used to document, standardize and control the naming and use of data?
- ☐ 9.2 Is access to the data dictionary restricted and monitored?
- ☐ 9.3 Are database maintenance utilities that bypass controls restricted and monitored for use?
- ☐ 9.4 If there is a software failure, is the system capable of automatically recovering the database?
- ☐ 9.5 Have automated or manual controls been implemented to protect against unauthorized disclosure of personal information?
- ☐ 9.6 Are methods in place to check and maintain the integrity of the data (for example consistency checks, checksums)?
- ☐ 9.7 Is there a vulnerability management program to monitor for alerts about new vulnerabilities and install patches in a timely manner?
- ☐ 9.8 Are default parameters on the database (for example accounts, passwords, etc.) changed frequently?
- ☐ 9.9 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 risk?

10. Transmission security

☐ 10.1 A public body or organization should consider whether it is appropriate to transmit personal information. Transmission includes speaking, email, messaging, faxing, file transfer protocols and any other way information can be passed from one point to another. If it decides to do so, is a policy in place that sets out policies and procedures that address which transmission medium to use for what personal information and how to use it?

☐ 10.2 Are regularly updated lists of fax numbers, email addresses and other contact information produced and distributed to ensure employees use current and accurate contact information when transmitting personal information?

10.3 When transmitting personal information, are the following steps taken to ensure that:

- ☐ The receiver is notified in advance of the transmission?
- ☐ The receiver stands by to receive the personal information and the location they are receiving the personal information is secure?
- ☐ The sender takes the utmost care to ensure they are transmitting the personal information to the correct destination?
- ☐ The transmission is encrypted?
- ☐ A confidentiality notice is attached, where possible?
- ☐ Pre-programmed contact information is regularly checked to ensure accuracy?
- ☐ Fax machines used to send or receive personal information are positioned in a secure area?
- ☐ Access to equipment used to send and receive personal information is controlled using access keys and passwords/pins?
- ☐ Transmission logs or activity history reports retained and checked for unauthorized transmissions?
- ☐ The internal hard drives and internal memory of transmission equipment are properly erased when disposing old equipment?
- ☐ Equipment used for the transmission and receipt of personal information are only used by authorized staff?

11. Data integrity and protection

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

- ☐ 11.1 Is there a procedure in place to ensure that any removal of personal information from the office premises has been properly authorized?
- ☐ 11.2 Is there an archiving process that ensures the secure storage of data, and guarantees the continued confidentiality, integrity and availability of the data?
- ☐ 11.3 Are encryption and other secure mechanisms in place for both the transport and storage of personal information?
- ☐ 11.4 Are automated or manual controls, or both, used to prevent unauthorized copying, transmission, or printing of personal information?
- ☐ 11.5 Are there policies and procedures in place to protect against unauthorized modification of data?
- ☐ 11.6 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 (for example digital signatures)?
- ☐ 11.7 Is there a process to revert and resolve changes if the data-integrity verification process fails?
- ☐ 11.8 Are file integrity monitoring tools (for example Tripwire) used to detect unexpected changes to files?

12. Access controls

General

- ☐ 12.1 Are there policies in place that require enhanced (multi-factor) authentication for privileged accounts?
- ☐ 12.2 Where appropriate, 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?
- ☐ 12.3 Are controls in place to detect any discrepancies in login attempts?

User registration, access and approval

- ☐ 12.4 Is a formal user registration and deregistration process in place?
- ☐ 12.5 Does the registration process include verification of user identity, verification and approval of access privileges, audit processes and actions to ensure access is not granted until approved?

- ☐ 12.6 Is each user of a system that processes personal information uniquely identified (no shared/generic accounts)?
- ☐ 12.7 Is the identification of the authorizer retained in the approval transaction record?
- ☐ 12.8 Is a current, accurate inventory of user accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts?

Roles

- ☐ 12.9 Is access control based on defined roles in your organization?
- ☐ 12.10 Are access privileges limited to the least amount of personal information required to carry out the role?
- ☐ 12.11 Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals?
- ☐ 12.12 Is there a clearly defined separation or segregation of duties (for example someone who initiates an event cannot authorize it) in the access management process?
- ☐ 12.13 Has the role been defined for managing access control on the various systems and platforms in the network?
- ☐ 12.14 Is a privacy officer role defined for all systems containing personal information that includes access control, data integrity, as well as backup and recovery?
- ☐ 12.15 Are roles and access rights for partners and third-party organizations (such as consultants, off-site storage) clearly defined?
- ☐ 12.16 Are access privileges allocated, modified or removed only after formal authorization?

Authentication

User authentication is the mechanism by which user identities are confirmed prior to granting access to a system.

- ☐ 12.17 Are the authentication mechanisms that are implemented commensurate with the sensitivity of the information and the associated risks (that is the more sensitive the information, the more robust the authentication mechanism)?
- ☐ 12.18 Are authentication codes or passwords generated, distributed and managed to maintain confidentiality and prevent unauthorized use?
- ☐ 12.19 Where authentication is based on username and password, are effective policies or controls in place to ensure robust passwords are used?

13. Acquisition, development and maintenance

- ☐ 13.1 Are security requirements identified as part of any new system development, acquisition or enhancement?
- ☐ 13.2 Does your organization have an asset management program that includes configuration management, problem management and change control processes (for example source code control, tickets and resolutions)?
- ☐ 13.3 Is there a patch management process for addressing security vulnerabilities?
- ☐ 13.4 Are there separate environments for development, testing and production?
- ☐ 13.5 Do the development and testing environments contain equivalent security controls to the production environment?
- ☐ 13.6 Are test datasets limited from containing real data except in situations where functional data cannot be manufactured?
- ☐ 13.7 Are development personnel restricted from having access to the production environment?
- ☐ 13.8 Is there a policy that prohibits the use of unauthorized software?
- ☐ 13.9 Are there controls that prevent or detect unauthorized software?
- ☐ 13.10 Are systems containing personal information maintained only by appropriately screened personnel?

14. Incident management

- ☐ 14.1 Is there a privacy and security incident management policy in place?
- ☐ 14.2 Does your organization have a framework for assessing the real risk of significant harm in the event of a privacy or security incident involving the loss, unauthorized access, or unauthorized disclosure of personal information?
- ☐ 14.3 Is there a formal Incident Response Plan for your organization?
- ☐ 14.4 Is there a designated individual or team responsible for incident response, and can they be assembled quickly?
- ☐ 14.5 Are there controls and procedures in place to ensure that security incidents (for example unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly?
- ☐ 14.6 Are there sufficient forensic capabilities available to allow investigators to collect the necessary evidence to successfully investigate?

☐ 14.7 Do incident management procedures include guidance for the capture and exchange of incident-related information with designated individuals and organizations in a timely fashion and in a manner that ensures documents related to the incident are protected from tampering?

14.8 Do the privacy incident management procedures include:

- ☐ Incident reporting and triage?
- ☐ Steps to asses and document the real risk of significant harm to individuals impacted by a security incident involving the loss, unauthorized access, or unauthorized disclosure of personal information?
- ☐ Containment, mitigation and recovery strategies?
- ☐ Notification and reporting requirements?
- ☐ Post-incident analysis ("lessons learned")?
- ☐ Prevention strategies?

☐ 14.9 Have your incident management procedures been endorsed by your senior management?

☐ 14.10 Are the individuals assigned to incident response roles adequately trained?

☐ 14.11 Are the incident response procedures reviewed and updated on a regular basis?

☐ 14.12 Does your organization keep and maintain a record of every incident involving the loss, unauthorized access, or unauthorized disclosure of personal information under its control?

☐ 14.13 Do these records include sufficient details (including, for example, the relevant security safeguards in place at the time) to explain how your organization determined whether a real risk of significant harm was a factor in these incidents?

☐ 14.14 Does your organization use a variety of mechanisms to continuously monitor and improve the operations of systems to detect anomalies in service delivery levels?

15. Business continuity planning

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

☐ 15.1 Is there a process in place to develop and maintain business continuity and disaster recovery throughout your organization?

☐ 15.2 Has your organization conducted an impact analysis to identify and prioritize the organization's critical services and assets?

☐ 15.3 Does the process include mechanisms to ensure that the cause of the interruption to business has been identified and documented?

15.4 Do the business continuity and disaster recovery plans address:

- ☐ Different levels of interruption of service?
- ☐ Physical damage?
- ☐ Environmental damage?
- ☐ Unauthorized modification or disclosure of information?
- ☐ Loss of control of system integrity?
- ☐ Physical theft?

☐ 15.5 Has your organization made provisions for the continuous review, testing and audit of business continuity and disaster recovery plans?

☐ 15.6 Have the plans been subject to appropriate organizational, departmental and regulatory expert review (for example legal, policy, finance, communications, information management and human resource specialists)?

☐ 15.7 Are backup processes in place to protect essential business information such as production servers, critical network components, software configurations, etc?

☐ 15.8 Are backups stored off site?

☐ 15.9 Are backup recovery procedures tested at regular intervals?

☐ 15.10 Where 100% availability is essential, are systems designed to be fully redundant with automated fail-over?

☐ 15.11 Are mechanisms in place to monitor your organization's level of overall readiness?

16. Compliance

Audit process design

☐ 16.1 Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?

☐ 16.2 Are all system audit logs that relate to the handling of personal information stored securely and monitored for tampering?

☐ 16.3 Are all audit logs that relate to the handling of personal information monitored through an automated anomaly detection system that generates alerts for review and action?

Ongoing audits

☐ 16.4 Are proactive audits conducted at regular intervals to verify the administrative and physical controls, integrity of the data, and discrepancies such as lost records or improper usage?

☐ 16.5 Is active monitoring in place to ensure that personal information cannot be passed between computers, or between discrete systems within the same computer, via unauthorized processes?

Scheduled audits

☐ 16.6 Are periodic audits performed to confirm asset inventory is maintained in an up-to-date fashion?

☐ 16.7 Is an annual physical inventory of all storage media containing personal information conducted and are discrepancies investigated immediately and corrected?

Audit verification

☐ 16.8 Are individuals who conduct audits able to access the assets they audit to satisfy themselves that the reports and similar materials they rely on to conduct the audit are accurate?

Audit recommendations

☐ 16.9 Do the management personnel responsible for the audit oversee the implementation of audit recommendations, verify completion of implementation and report verification results?