

PRIVACY CHECKUPS FOR ORGANIZATIONS IN THE GREATER VANCOUVER AREA

PREPARED FOR THE OFFICE OF THE
PRIVACY COMMISSIONER OF CANADA AND
FOR THE OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER OF BRITISH
COLUMBIA

March 25, 2009

3700 WILLINGDON AVENUE
BURNABY, BC V5G 3H2

CONTENTS	
Background	1
Approach	1
Conceptual Framework	2
Participation	4
Findings	5
<i>Protection of Personal Information against Unauthorized Access</i>	5
<i>Responding to Privacy Breaches</i>	8
Recommendations	8
Appendix 1: Field Interview/Inspection Questionnaire	11
Appendix 2: AICPA/CICA Generally Accepted Privacy Principles—Specimen Page	26

PRIVACY CHECKUPS

FOR ORGANIZATIONS IN THE GREATER VANCOUVER AREA

BACKGROUND

This report has been prepared pursuant to an agreement entered into under the Annual Privacy Research Contributions Program, which is funded by the Office of the Privacy Commissioner of Canada. The project that was undertaken is described on the Commissioner's website as follows:

Businesses collect and use information about their customers to improve service and gain a competitive advantage. However, mishandling this information can expose a company and its customers to serious risks. The Centre for Forensic and Security Technology Studies at British Columbia Institute of Technology will offer free "privacy protection checkups" to selected retail merchants, professional firms and non-profit organizations in the Lower Mainland of British Columbia. These checkups will provide organizations with a report on their compliance with privacy legislation and guidelines, as well as with recommendations for improvement where appropriate. The checkups will also serve as an opportunity to educate managers on their obligations to protect personal information.

APPROACH

Upon receiving funding approval, the Centre engaged the services of a number of students in its credential programs for the purpose of performing the privacy checkups. These students were provided with three days of training in issues surrounding privacy legislation, physical and technical security of personal information, identity fraud, and "best practices" regarding privacy protection. Presenters included representatives from the Office of the Information and Privacy Commissioner of B.C., the B.C. Crime Prevention Organization, and the private sector. Students were supplied with resource material to supplement the information presented at the training sessions.

Upon completion of the training sessions, a questionnaire/checklist was prepared for use as a framework in conducting the privacy checkups. A copy of this checklist appears in this report as Appendix 1. The students were then divided into two teams of three students each, with two students serving as spares. The project supervisor would make arrangements with a client organization for the conduct of a checkup and assign a team to perform the survey. Team members would obtain the required information by means of:

- Review of documents prepared by the client organization, and of its website

- Field visits to the client’s offices and interviews of client staff who are:
 - Responsible for development and maintaining policies and procedures for the protection of personal information and for compliance with privacy legislation;
 - Charged with the technical aspects of handling personal information; or
 - Handling personal information as part of their normal duties. In some cases, a representative sample of this group would be interviewed.
- “Walkabouts,” during which the team members would tour the client’s premises and take note of any issues that might compromise the security of personal information in the client’s possession or under the client’s control

On the basis of their information gathering, the students would prepare a draft report for review by the project supervisor. The supervisor would prepare a draft of a final report and circulate it to the team members for the purpose of ensuring that it accurately reflected their findings. The final report would then be transmitted to the representative of the client organization by email, in the form of a password-encrypted .pdf, and the password would be conveyed orally to the representative for added security.

CONCEPTUAL FRAMEWORK

The framework used in our assessments was the global privacy framework that was developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).¹ These “Generally Accepted Privacy Principles” were developed to “help management create an effective privacy program that addresses privacy risks and obligations and business opportunities.” The principles set out in this document are founded on key concepts from significant domestic and international privacy laws, regulations, and guidelines including Canada’s *Personal Information Protection and Electronic Documents Act* (PIPEDA).²

The principles included in this framework, together with the corresponding PIPEDA concepts, are set out in the following table.

¹ *Generally Accepted Privacy Principles; A Global Privacy Framework*. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, May 2006.

² *Idem*, pp. 60-62.

AICPA/CICA Generally Accepted Privacy Principle	PIPEDA CONCEPT
Principle 1: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures	Accountability
Principle 2: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.	Identifying Purposes, Openness
Principle 3: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.	Consent
Principle 4: The entity collects personal information only for the purposes identified in the notice.	Limiting Collection
Principle 5: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.	Limiting Use, Disclosure, and Retention
Principle 6: The entity provides individuals with access to their personal information for review and update.	Individual Access
Principle 7: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.	Limiting Use, Disclosure, and Retention
Principle 8: The entity protects personal information against unauthorized access (both physical and logical).	Safeguards
Principle 9: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.	Accuracy
Principle 10: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.	Challenging Compliance

Each of the GAPP principles is subdivided into two major areas:

- Policies and Communications
- Procedures and Controls

Under each of these sub-categories are listed a number of criteria, together with explanations and illustrations of these criteria and any additional considerations. A specimen page is attached to this report as Appendix 2.

As noted above, the principles in this framework have been mapped to the privacy legislation of Canada and other jurisdictions. For the purpose of our analysis, the feeling was that Principle 8 above was overly broad, since it embraces securing personal information against both physical and logical means of unauthorized access. Accordingly, our reporting on issues under this principle was subdivided into three aspects:

- General
- Physical
- Technical

Reports of our findings, presented to client organizations, were organized according to the principles noted above, with relevant issues noted under the appropriate principle.

PARTICIPATION

Clients for privacy checkups were solicited by contact with professional and business organizations, as well as by means of direct mailing to approximately 1,500 organizations on the mailing list of the Centre. Nevertheless, within the time allocated for the project, only eight organizations had expressed possible interest in receiving a privacy checkup, and only six of these ultimately agreed to participate.

Needless to say, this very low participation rate was extremely disappointing to the members of the team. Possible reasons for this apparent lack of interest have been suggested. These include:

- Unwillingness or inability to devote the required staff time to the exercise
- Fear that a checkup might result in adverse findings, which would, in turn, require action and expense to remedy
- Fear, despite assurances to the contrary, that possible adverse findings might be supplied to government authorities
- General lack of interest in issues related to privacy and to the protection of personal information

It is possible that an exploration of the reasons for the reluctance of organizations to participate may be an area for future research.

FINDINGS

Given the low participation rate in this study, it is not possible to present findings that lend themselves to statistical analysis. Nevertheless, some patterns emerged from our findings which are worth noting, since they may be helpful in directing future educational and awareness efforts. The pattern of privacy issues raised under each of the GAPP principles for each organization reviewed is displayed in Table 1

TABLE 1

NUMBER OF ISSUES		1	2	3	4	5	6	7	8 General	8 Physical	8 Technical	9	10	Total 1-10
GAPP Principle														
Organization 1	1	2	2	3	0	2	1	1	0	4	10	0	2	27
	2	0	1	1	0	2	1	0	5	5	6	0	1	22
	3	2	1	1	0	2	1	1	1	1	2	0	2	14
	4	0	0	3	0	1	1	0	1	4	5	0	1	16
	5	0	0	1	0	0	0	0	2	1	6	0	3	13
	6	2	1	0	0	0	2	1	0	2	8	0	1	17
Total Issues		6	5	9	0	7	6	3	9	17	37	0	10	109

It is apparent from this table that, overall, the surveyed organizations have relatively few issues identified under Principles 1-7. One reason for this may be the nature of the population surveyed. Of the six organizations that participated in the project, four were professional accounting firms. The professional association to which the partners of these firms belong has supplied its members with considerable information regarding their obligations under *PIPEDA*, as well as with templates, patterns of privacy policies, and discussions of best practices. In most cases, the accounting firms' policies and practices were in conformity with these guidelines. Because of this, and because of the nature of their business, our findings reflected a high degree of compliance with Principles 1-7.

PROTECTION OF PERSONAL INFORMATION AGAINST UNAUTHORIZED ACCESS

A major area of weakness for all organizations surveyed was Principle 8:

The entity protects personal information against unauthorized access (both physical and logical).

As indicated by Table 2, privacy issues raised under the three subdivisions of this Principle tended to be the most prevalent ones in each of the organizations surveyed.

TABLE 2³

PERCENTAGE OF ISSUES WITHIN EACH ORGANIZATION

GAPP Principle	1	2	3	4	5	6	7	8 General	8 Physical	8 Technical	9	10	Total 1-10
Organization 1	7%	7%	11%	0%	7%	4%	4%	0%	15%	37%	0%	7%	100%
2	0%	5%	5%	0%	9%	5%	0%	23%	23%	27%	0%	5%	100%
3	14%	7%	7%	0%	14%	7%	7%	7%	7%	14%	0%	14%	100%
4	0%	0%	19%	0%	6%	6%	0%	6%	25%	31%	0%	6%	100%
5	0%	0%	8%	0%	0%	0%	0%	15%	8%	46%	0%	23%	100%
6	12%	6%	0%	0%	0%	12%	6%	0%	12%	47%	0%	6%	100%

It is evident from the table above that:

- For every organization surveyed, the greatest number of privacy compliance issues raised were related to protection of information against unauthorized access; and
- Of the three subdivisions within this area, issues arising with regard to technical security were paramount

When these issues are expressed as a percentage of all issues raised for all organizations surveyed (Table 3, below), the figures are particularly striking. They confirm that the technical issues of privacy protection are the most significant gap in privacy compliance, with the physical security a second area of importance. By contrast, issues raised under other GAAP principles represent a relatively small proportion of the total.

TABLE 3⁴

PERCENTAGE OF OVERALL TOTAL ISSUES

GAPP Principle	1	2	3	4	5	6	7	8 General	8 Physical	8 Technical	9	10	Total 1-10
Organization 1	2%	2%	3%	0%	2%	1%	1%	0%	4%	9%	0%	2%	25%
2	0%	1%	1%	0%	2%	1%	0%	5%	5%	6%	0%	1%	20%
3	2%	1%	1%	0%	2%	1%	1%	1%	1%	2%	0%	2%	13%
4	0%	0%	3%	0%	1%	1%	0%	1%	4%	5%	0%	1%	15%
5	0%	0%	1%	0%	0%	0%	0%	2%	1%	6%	0%	3%	12%
6	2%	1%	0%	0%	0%	2%	1%	0%	2%	7%	0%	1%	16%
Total Issues	6%	5%	8%	0%	6%	6%	3%	8%	16%	34%	0%	9%	100%

The prevalence of issues associated with protection of personal information against unauthorized access appeared to be related to:

- General lack of awareness regarding physical security and technical security, and of the associated risks and exposures; and

³ Row totals do not add to manual percentage totals due to rounding error.

⁴ Row and column totals do not add to manual percentage totals due to rounding error.

- A tendency to contract out the technical aspects of information systems to external service firms without having sufficient contract controls in place, resulting in excessive reliance on external contractors for system development, architecture, maintenance, and assurance.

This finding is particularly troubling with regard to professional accounting firms. The reason for this is that accounting firms that prepare personal income tax returns routinely hold highly sensitive personal information about their clients, including:

- Name
- Address
- Marital status
- Date of birth
- Social Insurance number (SIN)
- Information regarding investments and other assets
- Information regarding income and sources of income, including employer information
- Identity and SIN of dependents

Compromise of this type of information could put clients at high risk of becoming the victims of identity theft, blackmail, or other criminal activities. Accordingly, our expectations for safeguarding client information were particularly high for this type of enterprise.

RESPONDING TO PRIVACY BREACHES

According to the Generally Accepted Privacy Principles⁵:

A privacy breach occurs when personal information is collected, retained, accessed, used, or disclosed in ways that are not in accordance with the provisions of the enterprise's policies, applicable privacy laws, or regulations.

The Generally Accepted Privacy Principles call for organizations to have a plan in place for the purpose of responding to privacy-breach incidents. Such plans would be expected to describe the process in a stepwise manner and set out responsibilities and timelines for containing the breach, evaluating the risks associated with the breach, notifying affected individuals, and preventing recurrences.

Our finding in this regard was that there was a very low level of compliance with this requirement. Where appropriate, the recommendations contained in our reports to management included a recommendation that such a plan be developed and documented, making reference to the checklists, templates, and other aids available for this purpose on the website of the Office of the Information and Privacy Commissioner of B.C.

RECOMMENDATIONS

In general, organizations surveyed had relatively few issues with regard to:

- Accountability for compliance with established privacy principles
- Identifying the purpose for which personal information is collected
- Obtaining consent for collection of personal information
- Limiting the collection of personal information to that which is necessary
- Limiting use, disclosure, and retention of personal information
- Maintaining accuracy, completeness, and currency of personal information
- Openness regarding information policies and practices
- Individual access to personal information

⁵ Page 58.

As noted in our findings above, this may be due in large part to the nature of the population surveyed, most of the organizations being professional firms that had been provided with model codes of practice by their professional association. Our impression was that substantially all of the issues arising under these headings could be addressed by minor changes to policy and practice, and by some further staff awareness training. Where appropriate, our reports to management included specific recommendations in this regard.

On the other hand, our survey did disclose a number of areas that represented significant compliance gaps. Although the number of organizations that participated in this project was limited, a number of clear patterns emerged:

1. Organizations overall are poorly prepared to protect personal information against unauthorized access, both physical and technical, with inadequacies in the area of technical security being particularly pronounced.
2. With regard to technical security, a major factor in the lack of appropriate policies and procedures was the practice of contracting out information-systems installation and maintenance to outside companies, and of relying upon these companies to implement and maintain information security measures without proper oversight and without sufficient, adequate communication between the organization and the contractor regarding what information security measures are required and what measures are in place. In most cases, critical information system features, including security features, were undocumented. This resulted in a lack of knowledge within the organizations regarding:
 - a. What security measures, if any, were in place
 - b. How, or if, such measures were monitored and maintained up to date
 - c. What corrective actions to take in the event of a security breach

In addition to the security concerns which are raised by this type of situation, there are also issues related to business continuity. In most cases, the external companies providing information systems service were small operations. In the event that such an operation were to go out of business and the principal to become unavailable for consultation, the organizations who had relied on these services might be unable to continue to implement necessary security measures or to recover from a critical system failure.

3. Organizations overall have not devoted appropriate attention to developing contingency plans to deal with privacy breaches, including the identification of specific staff responsibilities..

Based on these findings, we believe that the Office of the Information and Privacy Commissioner (B.C.) and the Office of the Privacy Commissioner (Canada) can play an important role in two distinct areas:

1. Personal Information Security

We recommend that the Commissions, preferably acting jointly, develop guidelines and training tools directed at organizations subject to PIPA, with regard to the physical and technical measures required to secure personal information effectively against unauthorized access. This would include the creation and dissemination of standards and “best practices” in these areas. In particular, guidelines should be developed for organizations to apply when using the services of external companies to develop, implement, and maintain all or part of their information systems.

2. Privacy Breach Preparedness

We recommend that the Commissions, again preferably working jointly, create guidelines and training tools to raise the awareness of organizations with regard to their obligation to have a contingency plan in place for dealing with breaches of privacy of personal information. Appropriate templates and models are already available,⁶ and efforts should be made to raise organizations’ awareness of them and to promote their use.

⁶ Organizations can find, on the website of the Office of the Information and Privacy Commissioner of B.C. , a privacy breach management policy template, a privacy breach checklist, and a breach notification assessment tool.

APPENDIX 1: FIELD INTERVIEW/INSPECTION QUESTIONNAIRE

OVERVIEW QUESTIONS

1. What personal information do you collect about your customers/clients? About your employees?

NOTE: A company might collect different sets of personal information for different purposes, particularly if it has different categories of customer or client. Document each such information set, and the related purposes. Example:

Name)

Address)

SIN) For personal income tax clients, in order to. . . .

Date of birth)

Name)

Address) For accounting for sole proprietorships

Bank name and account number)

2. What is the purpose of collecting this information?

3. How is this information collected?

- a. From the persons themselves?
 - i. Orally or in writing? By email? Etc.
- b. From third parties? Could include
 - i. Credit reporting agencies
 - ii. Former employers

4. If information is collected from third parties, how do you know that they are reliable sources? How do you know that the information was collected fairly, lawfully, and without deception?

5. Are technical means used to obtain personal information? Examples include:

- a. Internet forms
- b. Web beacons
- c. Cookies

6. When hiring employees, do you do background checks? How are these checks conducted?

7. Are your employees bonded?

8. What training do new employees receive regarding:

- a. Obligations under PIPA
- b. Effects of Social Engineering
- c. Importance of Privacy
- d. Liability Issues

9. Do you require new hires to sign a confidentiality agreement that includes their responsibilities under PIPA?

Note: Personal information includes, but is not limited to:

- ☑ Name*
- ☑ Address*
- ☑ Gender*
- ☑ Education*
- ☑ Income*
- ☑ S.I.N.*
- ☑ Birth date*
- ☑ Employment history*
- ☑ Medical history*
- ☑ Financial information*
- ☑ Credit card numbers*
- ☑ Driver's license number*
- ☑ Photographs*
- ☑ Vehicle information*

10. Do you have security/surveillance cameras on or around your premises? For what purpose? Overt and/or covert?

- a. Have you posted a clear and understandable notice about the use of cameras on your premises to individuals whose images might be captured by them, *before* these individuals enter the premises?
- b. Have you posted a contact in case individuals have questions or if they want access to images related to them? [*You may observe this*]
- c. How do you ensure that:
 - i. The recorded images are stored in a secure location, and access is granted only to a limited number of authorized individuals.
 - ii. Individuals have the right to access images relating to them. (*Note: When disclosing recordings to individuals who appear in them, the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.*)
 - iii. Any disclosure of video surveillance recordings outside the organization is justified and documented.
 - iv. Recordings are kept only as long as necessary to fulfill the purpose of the video surveillance.
 - v. Recordings no longer required (including backups) are securely destroyed.

11. Notes regarding employee information

- a. Do you ever receive unsolicited applications for employment and/or resumes? What do you do with them?
- b. When you are filling a position, what do you do with the information submitted by unsuccessful applicants?
- c. When checking on an applicant's information, do you contact the people on their

reference list? Do you contact people who may not be on their reference list? If so, do you take any steps to notify the applicant?

Principle 1: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures

Determine if the entity has a copy of the privacy policy. If it does, obtain a copy. This will be assessed using the criteria set out in your kit. If the entity does not have a policy, then advise the interviewee of the obligation of their organization to develop policies and procedures that are necessary for the organization to meet its obligations under PIPA, as well as a complaint process respecting the application of PIPA; and to make these available to individuals upon request. You may refer them to the OIPC website, where they can download guidelines for creating a privacy policy, as well as the text of a model policy.

Privacy Policies

1. Does your organization have a privacy policy? (obtain a copy)
2. Who is responsible for developing and maintaining privacy policy?
3. How often is the privacy policy reviewed? By whom?
4. Do you review your privacy policy and practices whenever there are changes in:
 - a. Business operations and processes
 - b. Technology or systems
 - c. Legislation
 - d. Contracts, including service-level agreements
5. Are your privacy policies and practices reviewed by a lawyer for compliance with PIPA?
6. How are employees made aware of this policy? Of changes in the policy?
7. Have you integrated your information management policies and practices into training for new staff?
8. How frequently are employees asked to review the policy?
9. Are employees required to confirm periodically their understanding of the policy and their agreement to its terms? Orally or in writing?
10. Are front-line staff trained to handle customer/client inquiries regarding
 - a. Privacy complaints
 - b. Correction requests
 - c. Requests for access to personal information

Responsibility and Accountability for Policies

11. Have you assigned accountability for privacy policies and practices to a designated individual or group of individuals (Privacy officer?)
12. Who are they?
13. Have you documented the responsibility of the accountable person(s)? For example, is it part of their job description?
14. How is the identity of the accountable person(s) made known to customers/clients? To employees?

Consistency of Commitments with Privacy Policies and Procedures

15. Do you use another organization to do work for you that involves personal information? For example, do you use another organization to process your payroll or your billings?

16. If so, is there an agreement in place that commits the organization providing services to adhere to your organization's privacy policy?

17. How do you ensure that the other organization is providing appropriate protection of the personal information that they receive from you? Do you have audit and enforcement mechanisms? Do you exercise them?

Principle 2: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

Obtain a copy of the privacy notice provided. Assess the content in view of:

the criteria, illustrations, explanations, and additional considerations in GAPP Principle 2, and in:

- GAPP 3.1.1
- GAPP 4.1.1
- GAPP 5.1.1
- GAPP 6.1.1
- GAPP 7.1.1
- GAPP 8.1.1
- GAPP 9.1.1.

Privacy Diagnostic Tool (PDT), Principle 2 (Identifying Purposes), p. 8-9

A Guide for Businesses and Organizations to the Personal Information Protection Act (PIPA Guide) (OPC website), p. 20

CICA Privacy Compliance—a Guide for Organizations & Assurance Practitioners (CICA Guide), p. 19-

If the organization has no written or web-present privacy notice, ask the following questions in addition to the ones below:

When you collect personal information from customers/clients or employees, do you let them know the purpose for which you're collecting it? Do you tell them in every case, or only if they ask?

What specifically do you tell them?

QUESTIONS FOR MANAGERS

1. How do you provide notice to your customers/clients and employees about your privacy policies and procedures? Printed form? Website?

2. Is the notice clearly dated?

3. Do you provide this information at or before the time you first collect personal information, or as soon as possible thereafter?

4. If your privacy policies or procedures change, how do you inform your existing customers/clients and employees?

Principle 3: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

Review the organization's privacy policy and notice in view of:

criteria, illustrations, explanations, and additional considerations in GAPP Principle 3

PIPA Guide, pp. 13-18

- ☐ PDT pp. 11-13
- ☐ GAPP Principle 3

1. When you collect personal information about customers/clients or employees, do you first obtain their consent? How do you obtain it? Is it written or oral? Email?
2. If consent is not given by the individual in person, how do you authenticate the identity of the person consenting?
3. What about when you obtain personal information about customers/clients or employees from a third person? Do you first obtain the consent of the customer/client or employee? (An example of third-person source might be obtaining a credit report for a customer or doing a background check on an employee or job candidate).
4. If consent is given by some means other than in writing (*e.g.* orally, over the Internet, by phone), how is this documented?
5. What effort do you make to advise the person of the purpose for which the information will be used?
6. What are the consequences if a person declines to consent to collection or use of their personal information? Do you advise them of the consequences?
7. Do you inform individuals that they may withdraw their consent at any time?
8. Do you periodically review and update the consent and withdrawal of consent for each individual?
9. Do you regularly review the customer/client consent *process*? How often?
10. Do you have a process in place to ensure that your employees collect only the information to which the customer has consented?
11. Do you periodically audit or review your staff's actions in obtaining customer/client consent to collect personal information?
12. Do you seek customer feedback regarding the clarity of your information and privacy policies, and their understanding of them?

Principle 4: The entity collects personal information only for the purposes identified in the notice.

The preliminary questions ask about the personal information that the organization collects, and the purpose for which it is collected. The privacy notice should also specify the purpose for which information is being gathered. In your review, determine whether the organization is collecting only the information required for the specified purposes. Thus, for example, a video rental store would not need a customer's driver's license number for the purpose of securing the return of rented videos.

QUESTIONS FOR MANAGEMENT:

1. Do you use and disclose the personal information that you collect only for the purposes for which you collected it?
2. If you use it for other purposes, do you first obtain consent?
3. Do you have procedures and technical measures in place to limit the use of information to the purposes for which it was collected? (Technical measure could include, for example, different levels of access authority to the computer system for different employees).
4. Are your employees aware of the limitations on the use and disclosure of personal

information?

5. Do you disclose personal information under your control to third parties? If so, do you do it for the purposes identified at the time that you collected it? If not, do you first obtain the consent of the individual?

Principle 5: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

1. Do you have an information-retention policy that specifies how long different classes of personal information are retained? Is this policy documented? May we have a copy?
2. Does this policy include retention of clients' payment card information (if applicable)?
3. How do you ensure that the information is not, in fact, being retained for an excessively long time?
4. Do you inform individuals about your retention periods and what is done with their information after the maximum retention period has been reached?
5. When you use personal information to make a decision about an individual, do you retain it long enough to allow the individual to access that information and to challenge its accuracy?
6. When personal information is no longer required, how do you go about disposing of it:
 - a. Paper (shredded?)
 - b. Electronic media (computer hard drives, PDA's, cell phones, flash drives, CD's, etc).
 - i. When disposing of computers, mobile or portable devices, and media that are no longer required, how do you protect the personal information that may be stored on them?
7. When disposing of personal information, how do you handle the information contained in archived or backup copies?
8. If you use a third party (*e.g.* a shredding service) to dispose of personal information, how do you ensure that it is disposed of appropriately?
9. How is personal information updated? What safeguards do you have in place to ensure that all updates to personal information are appropriately authorized? Do you take any measures to ensure that the updates are accurate?
10. Do you use offsite storage for any personal information? (This could include offsite storage of paper files or computer media, storage of files on external servers, etc.) If so, how do you ensure that this storage is secure? For example, are your archived electronic files encrypted?

Principle 6: The entity provides individuals with access to their personal information for review and update.

1. Are individuals made aware of their right to access their personal information under your control, and to challenge its accuracy and amend it? How are they made aware?
2. When an individual requests access to their personal information, how do you authenticate the identity of the requestor?
3. Can individuals access their personal information online? If so, what measures do you take to ensure that access to such information is authorized? (*e.g.* customer ID and password)
4. If an individual requests access to their personal information and you cannot find this information, what records do you keep to demonstrate that a diligent search was made.
5. Do you use unique client/customer identification numbers within your system? How are these identifiers assigned?

6. When sending a client/customer personal information by post, is the information mailed only to the address on record?
7. If an individual requests an address change, is confirmation of the change mailed to both the new and the old addresses?
8. Are they made aware of the process by which they can access their personal information?
9. When providing personal information to an individual in response to a request, in what form is it provided? Is it in a format that is generally understandable? If explanations are required to facilitate understanding (e.g. a list of the meaning of internal codes), do you supply it?
10. When responding to a request for access to personal information, do you:
 - a. Give the applicant access to the requested information in a timely manner?
 - b. Tell the applicant what the information has been, or is being, used for?
 - c. Tell the applicant to whom, and in what situations, the information is being, or has been, disclosed outside your organization?
11. When an individual requests access to their personal information, do you have a standard procedure for ensuring that all such personal information under your control, wherever located, is retrieved?
12. When providing an individual with access to their personal information under your control, do you include information in archived or backup systems or media?
13. On average, how long does it take your organization to respond to an individual's request for personal information? *NOTE: In BC, the entity must assist and respond within 30 business days.*
14. If it will take you longer than 30 business days to respond to a request for access to personal information, do you communicate with the individual? What do you tell them? *NOTE: PIPA requires that the individual be told why more time is required, when the request will be responded to, and that the individual has the right to complain to the Commissioner about the delay.*
15. Do you charge individuals for supplying them with their personal information? If so, how much do you charge?
16. Upon request, do you advise individuals how their personal information is being used and to whom it has been disclosed?
17. If you cannot supply a list of actual disclosures, do you supply a list of entities to which you *may have* disclosed their information?
18. How can individuals challenge the accuracy and completeness of their personal information under your control?
19. If you cannot agree to a requested correction, do you attach a statement of disagreement to the individual's records?
20. If you decide that there is no factual error or omission to correct, do you annotate the record with the requested correction that you did not make?
21. If you decide that there is no error or omission to correct do you:
 - a. Advise the individual of this fact
 - b. Advise the individual of their right to request the Commissioner to review your decision
 - c. Annotate the individual's record with the requested correction that you did not make and attach the request to the individual's record
22. When an individual's information is corrected, or a statement of disagreement is put on their records, do you send the corrected information or statement of disagreement to third parties to whom the personal information was previously disclosed? How do you identify such

third parties?

23. When preparing to provide an individual with access to their personal information, what measures do you take to ensure that the information that you disclose does not identify another person, either directly or indirectly?

24. Are you aware of the legal grounds upon which an individual may be denied access to their personal information under your control?

NOTE: In BC, these grounds include

Discretionary

- Legal privilege*
- Confidential commercial information*
- Collected for investigation or legal proceeding*
- Information would no longer be provided to the entity, and it is reasonable that it would be*
- Collected by a mediator or arbitrator under an agreement, Act, or by a court*
- Relates to or may be used in the exercise of prosecutorial discretion*

Mandatory

- Disclosure would threaten the life or security of another individual*
- Disclosure would reveal personal information about another individual and cannot reasonably be severed*
- The information would reveal the identity of someone who supplied information in confidence and cannot reasonably be severed*

25. If an individual's request for access to their personal information is denied in whole or in part, do you inform them in writing?

- a. Do you supply the reason that you are denying access?
- b. Do you supply a statutory reference for your reason?
- c. Do you supply the name of a person within the organization who can answer questions about the refusal?
- d. Do you advise the individual of their right to challenge this denial? *NOTE: Individuals can ask the Commissioner to review the organization's decision.*

26. If your organization receives a notice from another organization that an individual's personal information previously disclosed to you has been corrected, do you make the corresponding correction in your own records? How do you ensure that this is done?

27. How do you make your employees aware of the mechanism for handling client/customer requests for correction of personal information? For access to personal information? For handling disputes?

28. If a client/customer disputes your denial of a request for access to personal information, or a request to change personal information, how is this dispute documented?

Principle 7: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

1. What processes do you have in place to ensure that personal information is disclosed to third parties only for the purpose identified in your privacy notice, and with the consent of the individual?

2. What personal information do you routinely disclose to third parties as part of your business operation?
3. Do you have documented procedures for the approval of disclosure of personal information to third parties?
4. Have staff been trained in the appropriate way to handle non-routine requests for personal information?

Principle 8: The entity protects personal information against unauthorized access (both physical and logical).

General

1. Is the technical work on your information systems done in-house, or do you use an outside service?
2. If you use an outside service, what measures have you taken to ensure that the technicians are reliable?
3. Are your premises protected by an intrusion alarm? Is it monitored?

Information Security Program

1. Is there a member of your organization who has been assigned responsibility for security, including information security?
2. Do you have a security program that has been documented, approved, and implemented and that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction?
3. May we have a copy?
4. How does this program address the following issues:
 - a. Periodic risk assessments
 - b. Assignment of responsibility and accountability for security
 - c. Implementing system software upgrades and patches
 - d. Handling errors and omissions, security breaches, and other incidents
 - e. Procedures to detect actual and attempted attacks or intrusions into systems
 - f. Allocating training and other resources to support your organization's security policies
 - g. Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies
 - h. Disaster recovery planning and related testing
 - j. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts
 - k. Preclusion of access to personal information in computers, media, and paper-based information that is no longer in active use by the organization (e.g., computers, media and paper-based information in storage, sold, or otherwise disposed of).
 - i. How do you dispose of hard-copy records of personal information that are no longer needed
 - ii. When disposing of computers, mobile or portable devices, and media that are no longer required, how do you protect the personal information that may be stored on them?

Logical Access Controls

1. How do your logical access controls address the following issues:

- a. Authorizing and registering internal personnel and individuals
 - b. Identifying and authenticating internal personnel and individuals
 - c. Making changes and updating access profiles
 - d. Granting system access privileges and permissions
 - e. Preventing individuals from accessing other than their own personal or sensitive information
 - f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities
 - g. Distributing output only to authorized internal personnel
 - h. Restricting logical access to offline storage, backup data, systems, and media
 - i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls); and restriction of USB ports
 - j. Preventing the introduction of viruses, malicious code, and unauthorized software
 - k. Scheduled scanning for viruses, spyware, and other malware
 - l. Installation of the latest vendor-supplied security patches, virus definitions, and similar features for software applications (not system software)
 - m. Testing, evaluating, and authorizing system principles before implementation
 - n. Enhanced security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls.
2. Do you always have to login to any system using a unique identifier and password?
 3. Does the system force you to use a password that is complex (numbers, symbols, and letters in combination) and at least six characters in length?
 4. Does the system force you to change your password periodically? How often?
 5. Are all electronic files of personal information held on a secure server (that is, no personal information on a local hard drive)?
 6. Are office computer screens positioned to prevent unauthorized viewing?
 7. Have you set a screensaver to lock the system automatically after five minutes of inactivity?
 8. Wireless network—Routers:
 - a. Are they password protected?
 - b. Have manufacturer default settings been changed?
 - c. Are they backed up?
 - d. Who is responsible for maintaining upgrades and rules?
 9. Wireless network—are latest standards employed:
 - a. 802.11n - 100+ Mbps standard for Wi-Fi networks.
 - b. Replaces 802.11a, 802.11b and 802.11g standards for local area networking.
 - c. WEP - Wired Equivalent Privacy ? (NOTE—does not support high-level security)
 - d. WPA - Wi-Fi Protected Access
 10. Firewalls
 - a. Are they Password Protected
 - b. Have the Default Settings from the Manufacturer been changed?
 - c. Who has access to this information

- d. Are these backed up
- e. Who is responsible for maintaining upgrades and rules?

11. Network servers

- a. How often are security patches done?
- b. Has System Administrator been fully trained?
- c. How are multiple servers connected?
 - i. Hardwired
 - ii. Router
 - iii. Wireless.
- d. Are Audit trails maintained?
 - i. For network access
 - ii. For file access
 - iii. Internet access
 - iv. Intranet access.

12. Encryption

- a. What personal information is encrypted? On all media, including individual hard drives, servers, USB drives and backups?
- b. Type of encryption used. DES? AES?
- c. Where are encryption keys stored? Who has access to them?

Physical Access Controls (Note: include both paper copies and electronic files and media)

1. What systems do you have in place to:
 - i. Manage logical and physical access to personal information, including hard copy, archival, and backup copies.
 - ii. Log and monitor access to personal information.
 - iii. Prevent the unauthorized or accidental destruction or loss of personal information.
 - iv. Investigate breaches and attempts to gain unauthorized access.
 - v. Communicate investigation results to appropriate designated privacy executive.
 - vi. Maintain physical control over the distribution of reports containing personal information.
 - vii. Securely dispose of waste containing confidential information (for example, shredding).
2. Are paper files containing personal information stored in locked cabinets in a secure area? Are locks rated to an appropriate level of protection? (e.g. It is common to breach installed filing cabinet locks with a paper clip. Also, also certain padlocks such as Master can be easily comprised by knowing the padlock serial number.)
3. Are portable storage devices (e.g. USB drives) used? For what purpose? How is the information on them secured?
4. Do you always store any mobile or portable storage devices, including laptops, in a locked cabinet when they're not in use?
5. Is the personal information contained on portable storage devices:
 - i. Kept to a minimum
 - ii. Encrypted

iii. Securely deleted as soon as possible after use

- . Are laptops and other mobile or portable storage devices password protected?
- 7. When laptops are not locked away, are they secured by locks or alarms? What about when not at the office (e.g. at home or while travelling)?
- 8. Do your desktop computers that are not secured have removable hard drives? Where are they kept when not in use?
- 9. Are servers and other vital specialist equipment located in dedicated rooms with locked internal doors and no windows?
- 10. Are your staff instructed to check the backs of their desktops for keyloggers and other unauthorized devices on a regular basis? How frequently?

Environmental Factors

1. What measures do you have in place to protect against:
 - a. Fire
 - b. Flood
 - c. Dust
 - d. Power failure/surge
 - e. Excessive heat or humidity
 - f. Other environmental hazards

Note: Canvas both paper and electronic media here.

2. How frequently do you back up your data files that contain personal information?
3. Where are backups stored?
4. How have you ensured the security of information stored off-site?

Transmitted Personal Information

1. What measures do you take to secure personal information that is transmitted
 - a. by mail
 - b. over the Internet
 - c. over public networks (e.g. by fax)
 - d. by courier or other physical means
2. Have you set minimum level of encryption and controls of transmitted data (e.g. 128-bit SSL)?
3. When transmitting information by fax or email, do you ensure either that the owner of the information has consented to such transmission or that the information is encrypted?
4. Do you always attach a confidentiality notice to email and fax transmissions of personal information?
5. Before faxing personal information, do you:
 - a. Ensure that you are sending from a secure fax machine
 - b. Call the receiver to confirm that the receiving machine is secure, and to confirm the fax number
 - c. Use a cover sheet that includes the name and phone number of the sender and the intended recipient
 - d. Attach a confidentiality notice

Testing Security Safeguards

1. Are documented procedures in place to:
 - a. Regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information.
 - b. Periodically undertake independent audits of security controls using either internal or external auditors.
 - c. Test card access systems and other physical security devices at least annually.
 - d. Document and test disaster recovery and contingency plans at least annually to ensure their viability.
 - e. Periodically undertake threat and vulnerability testing, including security penetration reviews and Web vulnerability and resilience.
 - f. Make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities.

Compliance with Appropriate PCIDSS

If the organization takes debit or credit card payments, review the appropriate self-assessment questionnaire with the person responsible. Go over only the questionnaire proper (the part that makes reference to specific requirements).

Principle 9: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

NOTE: *In some cases, the information solicited below may already have been supplied as part of an earlier principle. If so, then you need not duplicate it here.*

1. What procedures do you have in place to verify and correct personal information?
2. Do you conduct periodic assessments of the accuracy of the personal information in your databases?
3. Do you keep the personal information under your control only as accurate, complete, and current as necessary for identified purposes? In other words, do you avoid collecting updated information unless it is required for the purpose that was identified when the information was first collected?
4. Are the limits to the requirement for accuracy clearly set out?
5. How do you ensure that the personal information under your control is sufficiently accurate, complete, and current to be used for its intended purpose?
6. Are individuals made aware of how they can update their personal information? How are they made aware?
7. Are systems and procedures in place to
 - a. Edit and validate personal information as it is collected, created, maintained, and updated.
 - b. Record the date when the personal information is obtained or updated.
 - c. Specify when the personal information is no longer valid.
 - d. Specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information).
 - e. Indicate how to verify the accuracy and completeness of personal information

obtained directly from an individual, received from a third party, or disclosed to a third party

Principle 10: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

1. Have you documented a response plan to deploy in the event of a breach of personal information? May we have a copy?
2. Does the plan include measures for:
 - a. Breach containment and preliminary assessment
 - b. Evaluation of the risks associated with the breach
 - c. Notification of individuals affected
 - d. Prevention of future breaches
 - e. Compliance with the Payment Card Industry Data Security Standard 12.9 and with cardholder-specific requirements
 - f. Annual testing
3. Do you have documented procedures in place for responding to complaints or inquiries about your handling of personal information?
4. Do these procedures enable you to:
 - a. Record and respond to all complaints in a timely manner.
 - b. Periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner.
 - c. Identify trends and the potential need to change the entity's privacy policies and procedures.
 - d. Address complaints that cannot be resolved.
5. How is information about your procedures conveyed to your employees? To your clients/customers?
6. Do you document all complaints received?
7. Do you investigate all complaints received?
8. Do you periodically review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts?
9. Are these reviews documented and followed up?
10. Regarding instances of non-compliance, are systems and procedures in place to:
 - a. Notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner.
 - b. Inform employees of the appropriate channels to report security vulnerabilities and privacy breaches.
 - c. Document instances of noncompliance with privacy policies and procedures.
 - d. Monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis.
 - e. Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers).
 - f. Identify trends that may require revisions to privacy policies and procedures.

PRIVACY ASSESSMENT WALKABOUT

While touring the premises, take note of the following:

PHYSICAL SECURITY

- Is any form of entrance control in place?
- Is there a system to log the entrance and leaving of employees? Of others?
- Are the premises laid out so that non-employee entrants are easily noticed?
- Are the premises monitored by CCTV (and, if so, is this posted)?
- Is there a staffed reception area?
- Are the premises guarded or patrolled during unoccupied hours?
- Are paper files containing personal information stored in:
 - o Areas that are inaccessible to non-employees
 - o Lockable and locked or otherwise access-controlled
 - o In locked file cabinets that are locked when not in use
- Are there exposed network cables?
- Are there loose ceiling tiles?
- Are plugs, cabling, and other wires protected from foot traffic?
- Are photocopiers and fax machines, and scanners kept in open view?

DESKTOPS AND WORK STATIONS

Look out for:

- Computer monitors visible from public areas with content displayed (not blacked out or covered by screen saver)
- Ports exposed to public access, enabling surreptitious attachment of unauthorized devices
 - Possible keylogger attached to cable
 - Passwords written down on or near computers
 - Computers unsecured by cable or other device
 - Storage media (CD, thumb drive, diskette, etc.) left loose and unattended
 - Documents and files that might contain personal information left unattended and/or visible from public areas
 - Phone conversations audible outside of immediate work area
 - Windows placed to allow public view of documents and/or computer monitor
 - Computer equipment not marked with ownership in an obvious and overt way

POS TERMINALS

Look out for:

- Terminals with no alarm or tamper-evident device (e.g. seal) or with device defaced
- Possible keylogger attached to cable
- Superfluous wires leading to the device
- Terminal in public area left unattended

APPENDIX 2: AICPA/CICA GENERALLY ACCEPTED PRIVACY PRINCIPLES—
SPECIMEN PAGE

Ref.	Collection Criteria	Illustrations and Explanations of Criteria	Additional Considerations
4.2 4.2.1	<p>Procedures and Controls</p> <p>Collection Limited to Identified Purpose</p> <p>The collection of personal information is limited to that necessary for the purposes identified in the notice.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> Specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information. Periodically review the entity's program or service needs for personal information (for example, once every five years or when there are changes to the program or service). Obtain explicit consent when sensitive personal information is collected (see 3.2.3, "Explicit Consent for Sensitive Information"). Monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such. 	
4.2.2	<p>Collection by Fair and Lawful Means</p> <p>Methods of collecting personal information are reviewed by management, legal counsel, or both before they are implemented to confirm that personal information is obtained:</p> <ul style="list-style-type: none"> Fairly, without intimidation or deception, and Lawfully, adhering to all relevant rules of law, whether derived from statute or common law. 	<p>The entity's legal counsel reviews the methods of collection and any changes thereto.</p>	<p>It may be considered a deceptive practice:</p> <ul style="list-style-type: none"> To use tools, such as cookies and Web beacons, on the entity's Web site to collect personal information without providing notice to the individual. To link information collected during an individual's visit to a Web site with personal information from other sources without providing notice to the individual.