Generally Accepted Privacy Principles

August 2009

Previously published by a legacy organization

Acknowledgments

The AICPA and Canadian Institute of Chartered Accountants (CICA) appreciate the contribution of the volunteers who devoted significant time and effort to this project. The institutes also acknowledge the support that the following organizations have provided to the development of *Generally Accepted Privacy Principles*:

- ISACA

- The Institute of Internal Auditors

Foreword

The AICPA and the Canadian Institute of Chartered Accountants (CICA) strongly believe that privacy is a business issue. Considering what organizations face when trying to address privacy issues, we quickly concluded that businesses did not have a comprehensive framework to manage their privacy risks effectively. The institutes decided that they could provide a significant contribution by developing a privacy framework that would address the needs of all of the parties affected by privacy requirements or expectations. Therefore, the institutes developed a privacy framework called AICPA and CICA *Generally Accepted Privacy Principles*. The institutes are making these principles and criteria widely available to all parties interested in addressing privacy issues.

These principles and criteria were developed and updated by volunteers who considered both current international privacy regulatory requirements and best practices. These principles and criteria were issued following the due process procedures of both institutes, which included exposure for public comment. The adoption of these principles and criteria is voluntary.

An underlying premise to these principles is that good privacy is good business. Good privacy practices are a key component of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information collected and held by an organization. As business systems and processes become increasingly complex and sophisticated, growing amounts of personal information are being collected. Because more data is being collected and held, most often in electronic format, personal information may be at risk to a variety of vulnerabilities, including loss, misuse, unauthorized access, and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments, individuals, and the public in general.

For organizations operating in a multijurisdictional environment, managing privacy risk can be an even more significant challenge. Adherence to generally accepted privacy principles does not guarantee compliance with all laws and regulations to which an organization is subject. Organizations need to be aware of the significant privacy requirements in all of the jurisdictions in which they do business. Although this framework provides guidance on privacy in general, organizations should consult their own legal counsel to obtain advice and guidance on particular laws and regulations governing an organization's specific situation.

With these issues in mind, the AICPA and CICA developed *Generally Accepted Privacy Principles* to be used as an operational framework to help management address privacy in a manner that takes into consideration many local, national, or international requirements. The primary objective is to facilitate privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy attestation engagement (usually referred to as a privacy audit) can be performed.

Generally Accepted Privacy Principles represents the AICPA and CICA contribution to aid organizations in maintaining the effective management of privacy risk, recognizing the needs of organizations, and reflecting the public interest. Additional history about the development and additional privacy resources can be found online at www.aicpa.org/privacy and www.cica.ca/privacy. *Generally Accepted Privacy Principles* can be downloaded from the AICPA and the CICA Web sites, at www.aicpa.org/privacy and www.cica.ca/privacy, respectively.

Because the privacy environment is constantly changing, *Generally Accepted Privacy Principles* will need to be revised from time to time; accordingly, please forward any comments about this document by email to the AICPA (GAPP@aicpa.org) or the CICA (privacy@cica.ca).

AICPA CICA

AICPA and CICA Privacy Task Force

Chair Everett C. Johnson, CPA *Deloitte & Touche LLP (retired)* **Vice Chair** Kenneth D. Askelson, CPA, CITP, CIA *JCPenney (retired)* Eric Federing *KPMG LLP* Philip M. Juravel, CPA *Juravel & Company, LLC* Sagi Leizerov, Ph.D., CIPP *Ernst & Young LLP* Rena Mears, CPA, CITP, CISSP, CISA, CIPP *Deloitte & Touche LLP* Robert Parker, FCA, CA·CISA, CMC *Deloitte & Touche LLP (retired)* Marilyn Prosch, Ph.D., CIPP *Arizona State University* Doron M. Rotman, CPA (Israel), CISA, CIA, CISM, CIPP *KPMG LLP* Kerry Shackelford, CPA *KLS Consulting LLC* Donald E. Sheehy, CA·CISA, CIPP/C *Deloitte & Touche LLP*	**Staff Contact:** Nicholas F. Cheung, CA, CIPP/C CICA *Principal, Assurance Services Development* Bryan Walker, CA CICA *Director, Practitioner Support* Nancy A. Cohen, CPA, CITP, CIPP AICPA *Senior Technical Manager, Specialized Communities and Practice Management* James C. Metzler, CPA, CITP AICPA *Vice President, Small Firm Interests* The AICPA Assurance Services Executive Committee approved *Generally Accepted Privacy Principles* in August 2009.

Table of Contents

Privacy—An Introduction to Generally Accepted Privacy Principles

Introduction

Many organizations find challenges in managing privacy[1] on local, national, or international bases. Most are faced with a number of differing privacy laws and regulations whose requirements need to be operationalized.

Generally Accepted Privacy Principles (GAPP) has been developed from a business perspective, referencing some, but by no means all, significant local, national, and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. Illustrative policy requirements, communications, and controls, including monitoring controls, are provided as support for the criteria.

GAPP can be used by any organization as part of its privacy program. GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations, and business opportunities. It can also be a useful tool to boards and others charged with governance and providing oversight. This introduction includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated is how these principles can be applied to outsourcing scenarios and the potential types of privacy initiatives that can be undertaken for the benefit of organizations and their customers.

This introduction and the set of privacy principles and related criteria that follow will be useful to those who

- oversee and monitor privacy and security programs.
- implement and manage privacy in an organization.
- implement and manage security in an organization.
- oversee and manage risks and compliance in an organization.
- assess compliance and audit privacy and security programs.
- regulate privacy.

1 The first occurrence of each word contained in appendix A—Glossary is underlined and hyperlinked back to its definition in the glossary in the introduction section and in the *Generally Accepted Privacy Principles* and related criteria tables.

Why Privacy Is a Business Issue

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, organizations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access, and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. Governments are trying to protect the public interest and, at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information, and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access to personal information, especially financial and medical records, and information about children.

Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, all businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures:

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

International Privacy Considerations

For organizations operating in more than one country, the management of their privacy risk can be a significant challenge.

For example, the global nature of the Internet and business means regulatory actions in one country may affect the rights and obligations of individual users and customers around the world. Many countries have laws regulating transborder data flow, including the European Union's (EU) directives on data protection and privacy, with which an organization must comply if it wants to do business in those countries. Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it.

In addition, organizations are challenged to try and stay up to date with the requirements for each country in which they do business. By adhering to a high global standard, such as those set out in this document, compliance with many regulations will be facilitated.

Even organizations with limited international exposure often face issues of compliance with privacy requirements in other countries. Many of these organizations are unsure how to address often stricter overseas regulations. This increases the risk that an organization inadvertently could commit a breach that becomes an example to be publicized by the offended host country.

Furthermore, many local jurisdictions (such as states or provinces) and certain industries, such as healthcare or banking, have specific requirements related to privacy.

Outsourcing and Privacy

Outsourcing increases the complexity for dealing with privacy. An organization may outsource a part of its business process and, with it, some responsibility for privacy; however, the organization cannot outsource its ultimate responsibility for privacy for its business processes. Complexity increases when the entity that performs the outsourced service is in a different country and may be subject to different privacy laws or perhaps no privacy requirements at all. In such circumstances, the organization that outsources a business process will need to ensure it manages its privacy responsibilities appropriately.

GAPP and its supporting criteria can assist an organization in completing assessments (including independent examinations) about the privacy policies, procedures, and practices of the third party providing the outsourced services.

The fact that these principles and criteria have global application can provide comfort to an outsourcer that privacy assessments can be undertaken using a consistent measurement based on internationally known fair information practices.

What Is Privacy?

Privacy Definition

Privacy is defined in *Generally Accepted Privacy Principles* as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information."

Personal Information

Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements. For additional information on criteria for confidentiality, refer to the AICPA and CICA *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (see www.aicpa.org/TrustServices or www.webtrust.org).

Introducing Generally Accepted Privacy Principles

GAPP is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities.

The privacy principles and criteria are founded on key concepts from significant local, national, and international privacy laws, regulations, guidelines,[2] and good business practices. By using GAPP, organizations can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. GAPP also facilitates the management of privacy risk on a multijurisdictional basis.

Overall Privacy Objective

The privacy principles and criteria are founded on the following privacy objective.

Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in *Generally Accepted Privacy Principles* issued by the AICPA and CICA.

Generally Accepted Privacy Principles

The privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

---

[2] For example, the Organisation for Economic Co-operation and Development has issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European Union has issued Directive on Data Privacy (Directive 95/46/EC). In addition, the United States has enacted the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act. Canada has enacted the Personal Information Protection and Electronic Documents Act and Australia has enacted the Australian Privacy Act of 1988, as amended in 2001. A chart comparing these international privacy concepts with generally accepted privacy principles can be found online at www.aicpa.org/privacy. Compliance with this set of generally accepted privacy principles and criteria may not necessarily result in compliance with applicable privacy laws and regulations, and entities should seek appropriate legal advice regarding compliance with any laws and regulations.

The following are the 10 *generally accepted privacy principles*:

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** 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.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** 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 or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** 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.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been specified to guide the development and evaluation of an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and standards. *Communications* refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice

and its commitments therein and other relevant information. *Procedures and controls* are the other actions the organization takes to achieve the criteria.

Using GAPP

GAPP can be used by organizations for the following:

- Designing, implementing, and communicating privacy policy
- Establishing and managing privacy programs
- Monitoring and auditing privacy programs
- Measuring performance and benchmarking

Establishing and managing a privacy program involves the following activities:

Strategizing. Performing privacy strategic and business planning.
Diagnosing. Performing privacy gap and risk analyses.
Implementing. Developing, documenting, introducing, and institutionalizing the program's action plan, including establishing controls over personal information.
Sustaining and managing. Monitoring activities of a privacy program.
Auditing. Internal or external auditors evaluating the organization's privacy program.

The following table summarizes and illustrates how GAPP can be used by an organization to address these business activities.

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
Strategizing	**Vision.** An entity's strategy is concerned with its long-term direction and prosperity. The vision identifies the entity's culture and helps shape and determine how the entity will interact with its external environment, including customers, competitors, and legal, social, and ethical issues. **Strategic Planning.** This is an entity's overall master plan, encompassing its strategic direction. Its objective is to ensure that the entity's efforts are all headed in a common direction. The strategic plan identifies the entity's long-term goals	**Vision.** Within an entity's privacy effort, establishing the vision helps the entity integrate preferences and prioritize goals. **Strategic Planning.** Within an entity's privacy effort, *Generally Accepted Privacy Principles* (GAPP) can be used to assist the organization in identifying significant components that need to be addressed.

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	and major issues for becoming privacy compliant. **Resource Allocation.** This step identifies the human, financial, and other resources allocated to achieve the goals and objectives set forth in the strategic plan or business plan.	 **Resource Allocation.** Using GAPP, the entity would identify the people working with and responsible for areas that might include systems management, privacy and security concerns, and stipulate the resourcing for their activities. **Overall Strategy.** A strategic document describes expected or intended future development. GAPP can assist an entity in clarifying plans for the systems under consideration or for the business's privacy objectives. The plan identifies the process to achieve goals and milestones. It also provides a mechanism to communicate critical implementation elements, including details on services, budgets, development costs, promotion, and privacy advertising.
Diagnosing	This stage, often referred to as the assessment phase, encompasses a thorough analysis of the entity's environment, identifying opportunities where weaknesses, vulnerability, and threats exist. The most common initial project for an organization is a diagnostic assessment. The purpose of such an assessment is to evaluate the entity against its privacy goals and objectives and determine to what extent the organization is achieving those goals and objectives.	GAPP can assist the entity in understanding its high-level risks, opportunities, needs, privacy policy and practices, competitive pressures, and the requirements of the relevant laws and regulations to which the entity is subject. GAPP provides a legislative neutral benchmark to allow the entity to assess the current state of privacy against the desired state.
Implementing	At this point, an action plan is mobilized or a diagnostic recommendation is put into effect, or both. Implementing involves developing and documenting a privacy program and action plan and the execution of all planned and other tasks necessary to make the action plan operational. It includes defining	GAPP can assist the entity in meeting its implementation goals. At the completion of the implementation phase, the entity should have developed the following deliverables: • Systems, procedures, and processes to address the privacy

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	who will perform what tasks, assigning responsibilities, and establishing schedules and milestones. This involves the planning and implementation of a series of planned projects to provide guidance, direction, methodology, and tools to the organization in developing its initiatives.	requirements • Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs
Sustaining and managing	Sustaining and managing involves monitoring the work to identify how progress differs from the action plan in time to initiate corrective action. Monitoring refers to the management policies, processes, and supporting technology to ensure compliance with organizational privacy policies and procedures and the ability to exhibit due diligence.	The entity can use GAPP to develop appropriate reporting criteria for monitoring requests for information, the sources used to compile the information and the information actually disclosed. It can also be used for determining validation procedures to ensure that the parties to whom the information was disclosed are entitled to receive that information.
Internal privacy audit	Internal auditors provide objective assurance and consulting services designed to add value and improve an entity's operations. They help an entity accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.	Internal auditors can evaluate an entity's privacy program and controls using GAPP as a benchmark and provide useful information and reporting to management.
External privacy audit	External auditors, notably certified public accountants (CPAs) and chartered accountants (CAs), can perform attestation and assurance services. Generally, these services, whether performed on financial and nonfinancial information, build trust and confidence for individuals, management, customers, business partners, and other users.	An external auditor can evaluate an entity's privacy program and controls in accordance with GAPP and provide reports useful to individuals, management, customers, business partners, and other users.

Presentation of Generally Accepted Privacy Principles and Criteria

Under each principle, the criteria are presented in a three column format. The first column contains the measurement criteria. The second column contains illustrative controls and procedures, which are designed to provide examples and enhance the understanding of how the criteria might be applied. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that may pertain to a certain industry or country.

Some of the criteria may not be directly applicable to some organizations or some processes. When a criterion is considered not applicable, the entity should consider justifying that decision to support future evaluation.

These principles and criteria provide a basis for designing, implementing, maintaining, evaluating, and auditing a privacy program to meet an entity's needs.

Generally Accepted Privacy Principles and Criteria

Management

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
1.0	**The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**		
1.1	**Policies and Communications**		
1.1.0	**Privacy Policies** The entity defines and documents its privacy policies with respect to the following: *a.* Notice (See 2.1.0) *b.* Choice and consent (See 3.1.0) *c.* Collection (See 4.1.0) *d.* Use, retention, and disposal (See 5.1.0) *e.* Access (See 6.1.0) *f.* Disclosure to third parties (See 7.1.0) *g.* Security for privacy (See 8.1.0) *h.* Quality (See 9.1.0) *i.* Monitoring and enforcement (See 10.1.0)	Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.	
1.1.1	**Communication to Internal Personnel** Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy	The entity • periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies. Changes to its privacy policies are communicated shortly after approval.	Privacy policies (as used herein) include security policies relevant to the protection of personal information.

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
	policies are communicated to such personnel shortly after the changes are approved.	• requires internal personnel to confirm (initially and periodically) their understanding of the entity's privacy policies and their agreement to comply with them.	
1.1.2	**Responsibility and Accountability for Policies** Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	The entity assigns responsibility for privacy policies to a designated person, such as a corporate privacy officer. (Those assigned responsibility for privacy policies may be different from those assigned for other policies, such as security). The responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include the following: • Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required • Formulating and maintaining the entity's privacy policies • Monitoring and updating the entity's privacy policies • Delegating authority for enforcing the entity's privacy policies • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices A committee of the board of directors	The individual identified as being accountable for privacy should be from within the entity.

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		includes privacy periodically in its regular review of overall corporate governance.	
1.2	**Procedures and Controls**		
1.2.1	**Review and Approval** Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Privacy policies and procedures are • reviewed and approved by senior management or a management committee. • reviewed at least annually and updated as needed.	
1.2.2	**Consistency of Privacy Policies and Procedures With Laws and Regulations** Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Corporate counsel or the legal department • determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates. • identifies other standards applicable to the entity. • reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws, regulations, and appropriate standards.	In addition to legal and regulatory requirements, some entities may elect to comply with certain standards, such as those published by International Organization for Standardization (ISO), or may be required to comply with certain standards, such as those published by the payment card industry, as a condition of doing business. Entities may include such standards as part of this process.
1.2.3	**Personal Information Identification and Classification** The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.	The entity has both an information classification policy and process, which include the following: • A classification process, which identifies and classifies information into one or more of the following categories: — Business confidential — Personal information (sensitive and other personal information) — Business general	

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		— Public • Identifying processes, systems, and third parties that handle personal information • Specific security and privacy policies and procedures that apply to each category of information	
1.2.4	**Risk Assessment** A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.	A process is in place to periodically identify the risks to the entity's personal information. Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as e-mailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. The process considers factors such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities.	Ideally, the privacy risk assessment should be integrated with the security risk assessment and be a part of the entity's overall enterprise risk management program. The board or a committee of the board should provide oversight and review of the privacy risk assessment.
1.2.5	**Consistency of Commitments With Privacy Policies and Procedures** Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Both management and the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.	
1.2.6	**Infrastructure and Systems Management** The potential privacy impact is	The following are used for addressing privacy impact: • Management assesses the	Some jurisdictions prohibit the use of personal information for test and development purposes unless it has

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
	assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following: — Infrastructure — Systems — Applications — Web sites — Procedures — Products and services — Data bases and information repositories — Mobile computing and other similar electronic devices The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.	privacy impact of new and significantly changed products, services, business processes, and infrastructure. • The entity uses a documented systems development and change management process for all information systems and related technology (including manual procedures, application programs, technology infrastructure, organizational structure, and the responsibilities of users and systems personnel), used to collect, use, retain, disclose, and destroy personal information. • The entity assesses planned new systems and changes for their potential effect on privacy. • Changes to system components are tested to minimize the risk of any adverse effect on the protection of personal information. All test data are anonymized. A controlled test database is maintained for full regression testing to ensure that changes to one program do not adversely affect other programs that process personal information. • Procedures ensure the maintenance of integrity and protection of personal information during migration from old to new or changed systems. • Documentation and approval by	been anonymized or otherwise protected to the same level required in its policies for production information.

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		the privacy officer, security officer, business unit manager, and IT management are required before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes are required to maintain the same level of protection of personal information; however, they may be documented and approved on an after-the-fact basis. The IT function maintains a listing of all software that processes personal information and the respective level, version, and patches that have been applied. Procedures exist to provide that only authorized, tested, and documented changes are made to the system. Where computerized systems are involved, appropriate procedures are followed, such as the use of separate development, test, and production libraries to ensure that access to personal information is appropriately restricted. Personnel responsible for initiating or implementing new systems and changes, and users of new or revised processes and applications, are provided training and awareness sessions related to privacy. Specific roles and responsibilities are assigned	

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		related to privacy.	
1.2.7	**Privacy Incident and Breach Management** A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management, and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholders breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate • A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following: — Incident patterns and root cause — Changes in the internal control environment or external requirements (regulation or legislation) • Periodic testing or walkthrough process (at least on an annual	A formal, comprehensive privacy incident and breach management program has been implemented, which specifies the following: • Incidents and breaches are reported to a member of the breach team, who assesses if it is privacy or security related, or both, classifies the severity of the incident, initiates required actions, and determines the required involvement by individuals who are responsible for privacy and security. • The chief privacy officer (CPO) has the overall accountability for the program and is supported by the privacy and security steering committees and assisted by the breach team. Incidents and breaches that do not involve personal information are the responsibility of the chief security officer. • The entity has a privacy breach notification policy, supported by (*a*) a process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach, (*b*) a process for assessing the need for stakeholders breach notification, if required by law, regulation, or policy, and (*c*) a process for delivering the notice in a timely manner. The entity	Some entities may adopt a breach notification policy for consistent use across all jurisdictions in which they operate. By necessity, such a policy would, at a minimum, be based on the most comprehensive legal requirements in any such jurisdiction.

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
	basis) and associated program remediation as needed	has agreements in place with a third party to manage the notification process and provide credit monitoring services for individuals, if needed. • The program includes a clear escalation path, based on the type or severity, or both, of the incident, up to executive management, legal counsel, and the board. • The program sets forth a process for contacting law enforcement, regulatory, or other authorities when necessary. • Program training for new hires and team members, and awareness training for general staff, is conducted annually, when a significant change in the program is implemented, and after any major incident. The privacy incident and breach management program also specifies the following: • After any major privacy incident, a formal incident evaluation is conducted by internal audit or outside consultants. • A quarterly review of actual incidents is conducted and required program updates are identified based on the following: — Incident root cause — Incident patterns — Changes in the internal control environment and legislation	

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		• Results of the quarterly review are reported to the privacy steering committee and annually to the audit committee. • Key metrics are defined, tracked and reported to senior management on a quarterly basis. • The program is tested at least every six months and shortly after the implementation of significant system or procedural changes.	
1.2.8	**Supporting Resources** Resources are provided by the entity to implement and support its privacy policies.	Management annually reviews the assignment of personnel, budgets, and allocation of other resources to its privacy program.	
1.2.9	**Qualifications of Internal Personnel** The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.	The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as the following: • Formal job descriptions (including responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions) • Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) and formal employment and confidentiality agreements • Performance appraisals (performed by supervisors, including assessments of	

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
		professional development activities)	
1.2.10	**Privacy Awareness and Training** A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.	An interactive online privacy and security awareness course is required annually for all employees. New employees, contractors, and others are required to complete this course within the first month following employment in order to retain their access privileges. In-depth training is provided which covers privacy and relevant security policies and procedures, legal and regulatory considerations, incident response, and related topics. Such training is • required annually for all employees who have access to personal information or are responsible for protection of personal information. • tailored to the employee's job responsibilities. • supplemented by external training and conferences. Attendance at the entity's privacy training and awareness courses is monitored. Training and awareness courses are reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements.	

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
1.2.11	**Changes in Regulatory and Business Requirements** For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed: — Legal and regulatory — Contracts, including service-level agreements — Industry requirements — Business operations and processes — People, roles, and responsibilities — Technology Privacy policies and procedures are updated to reflect changes in requirements.	The entity has an ongoing process in place to monitor, assess, and address the effect on privacy requirements from changes in the following: • Legal and regulatory environments • Industry requirements (such as those for the Direct Marketing Association) • Contracts, including service-level agreements with third parties (changes that alter the privacy and security related clauses in contracts are reviewed and approved by the privacy officer or legal counsel before they are executed) • Business operations and processes • People assigned responsibility for privacy and security matters • Technology (prior to implementation)	Ideally, these procedures would be coordinated with the risk assessment process. The entity also should consider emerging and good practices, such as breach notification in jurisdictions where none is required.

Notice

Ref.	Notice Criteria	Illustrative Controls and Procedures	Additional Considerations
2.0	**The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.**		
2.1	**Policies and Communications**		
2.1.0	**Privacy Policies** The entity's privacy policies address providing notice to individuals.		
2.1.1	**Communication to Individuals** Notice is provided to individuals regarding the following privacy policies: *a.* Purpose for collecting personal information *b.* Choice and consent (See 3.1.1) *c.* Collection (See 4.1.1) *d.* Use, retention, and disposal (See 5.1.1) *e.* Access (See 6.1.1) *f.* Disclosure to third parties (See 7.1.1) *g.* Security for privacy (See 8.1.1) *h.* Quality (See 9.1.1) *i.* Monitoring and enforcement (See 10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.	The entity's privacy notice • describes the personal information collected, the sources of such information, and purposes for which it is collected. • indicates the purpose for collecting sensitive personal information and whether such purpose is part of a legal requirement. • describes the consequences, if any, of not providing the requested information. • indicates that certain information may be developed about individuals, such as buying patterns. • may be provided in various ways (for example, in a face-to-face conversation, on a telephone interview, on an application form or questionnaire, or electronically). However, written notice is the preferred method.	Notice also may describe situations in which personal information will be disclosed, such as the following: • Certain processing for purposes of public security or defense • Certain processing for purposes of public health or safety • When allowed or required by law The purpose described in the notice should be stated in such a manner that the individual can reasonably understand the purpose and how the personal information is to be used. Such purpose should be consistent with the business purpose of the entity and not overly broad. Consideration should be given to providing a summary level notice with links to more detailed sections of the policy.
2.2	**Procedures and Controls**		
2.2.1	**Provision of Notice**	The privacy notice is	See 3.2.2, "Consent for New Purposes

Ref.	Notice Criteria	Illustrative Controls and Procedures	Additional Considerations
	Notice is provided to the individual about the entity's privacy policies and procedures (*a*) at or before the time personal information is collected, or as soon as practical thereafter, (*b*) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.	• readily accessible and available when personal information is first collected from the individual. • provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity. • clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity • tracks previous iterations of the entity's privacy policies and procedures. • informs individuals of a change to a previously communicated privacy notice, for example, by posting the notification on the entity's Web site, by sending written notice via postal mail, or by sending an e-mail. • documents that changes to privacy policies and procedures were communicated to individuals.	and Uses." Some regulatory requirements indicate that a privacy notice is to be provided on a periodic basis, for example, annually in the Gramm-Leach-Bliley Act (GLBA).
2.2.2	**Entities and Activities Covered** An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.	The privacy notice describes the particular entities, business segments, locations, and types of information covered, such as: • Operating jurisdictions (legal and	

Ref.	Notice Criteria	Illustrative Controls and Procedures	Additional Considerations
		political) • Business segments and affiliates • Lines of business • Types of third parties (for example, delivery companies and other types of service providers) • Types of information (for example, information about customers and potential customers) • Sources of information (for example, mail order or online) The entity informs individuals when they might assume they are covered by the entity's privacy policies but, in fact, are no longer covered (for example, linking to another Web site that is similar to the entity's, or using services on the entity's premises provided by third parties).	
2.2.3	**Clear and Conspicuous** The entity's privacy notice is conspicuous and uses clear language.	The privacy notice is • in plain and simple language. • appropriately labeled, easy to see, and not in unusually small print. • linked to or displayed on the Web site at points of data collection. • available in the national languages used on the site or in languages required by law.	If multiple notices are used for different subsidiaries or segments of an entity, similar formats are encouraged to avoid consumer confusion and allow consumers to identify any differences. Some regulations may contain specific information that a notice must contain. Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure.

Choice and Consent

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
3.0	**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.**		
3.1	**Policies and Communications**		
3.1.0	**Privacy Policies** The entity's privacy policies address the choices available to individuals and the consent to be obtained.		
3.1.1	**Communication to Individuals** Individuals are informed about (*a*) the choices available to them with respect to the collection, use, and disclosure of personal information, and (*b*) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.	The entity's privacy notice describes, in a clear and concise manner, the following: • The choices available to the individual regarding the collection, use, and disclosure of personal information • The process an individual should follow to exercise these choices (for example, checking an opt out box to decline receiving marketing materials) • The ability of, and process for, an individual to change contact preferences • The consequences of failing to provide personal information required for a transaction or service Individuals are advised of the following: • Personal information not essential to the purposes identified in the privacy notice	Some laws and regulations (such as Principle 11, "Limits on disclosure of personal information," section 1 of the Australian Privacy Act of 1988) provide specific exemptions for the entity not to obtain the individual's consent. Examples of such situations include the following: • The record keeper believes, on reasonable grounds, that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. • Use of the information for that other purpose is required or authorized by or under law.

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
		need not be provided. • Preferences may be changed, and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice. The type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the entity).	
3.1.2	**Consequences of Denying or Withdrawing Consent** When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	At the time of collection, the entity informs individuals of the following: • About the consequences of refusing to provide personal information (for example, transactions may not be processed) • About the consequences of denying or withdrawing consent (for example, opting out of receiving information about products and services may result in not being made aware of sales promotions) • About how they will or will not be affected by failing to provide more than the minimum required personal information (for example, services or products will still be provided)	
3.2	**Procedures and Controls**		
3.2.1	**Implicit or Explicit Consent**	The entity	

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
	Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.	• obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is collected or soon after). • confirms an individual's preferences (in writing or electronically). • documents and manages changes to an individual's preferences. • ensures that an individual's preferences are implemented in a timely fashion. • addresses conflicts in the records about an individual's preferences by providing a process for users to notify and challenge a vendor's interpretation of their contact preferences. • ensures that the use of personal information, throughout the entity and by third parties, is in accordance with an individual's preferences.	
3.2.2	**Consent for New Purposes and Uses** If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	When personal information is to be used for a purpose not previously specified, the entity • notifies the individual and documents the new purpose. • obtains and documents consent or withdrawal of consent to use the personal information for the new purpose. • ensures that personal information is being used in accordance with the new purpose	

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
		or, if consent was withdrawn, not so used.	
3.2.3	**Explicit Consent for Sensitive Information** Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	The entity collects sensitive information only if the individual provides explicit consent. *Explicit consent* requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.	Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1, clause 4.3.6, states that an organization should generally seek explicit consent when the information is likely to be considered sensitive. Many jurisdictions prohibit the collection of sensitive data, unless specifically allowed. For example, in the EU member state of Greece, Article 7 of Greece's "Law on the protection of individuals with regard to the processing of personal data" states, "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained. Some jurisdictions consider government-issued personal identifiers, for example, Social Security numbers or Social Insurance numbers, to be sensitive information.
3.2.4	**Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices** Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.	The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer or other similar electronic device. If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that	Consideration should be given to prevent or detect the introduction of software that is designed to mine or extract information from a computer or other similar electronic device and therefore may be used to extract personal information, for example, spyware.

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
		cookies are not stored on the customer's computer or other similar electronic device. Entities will not download software that will transfer personal information without obtaining permission.	

Collection

Ref.	Collection Criteria	Illustrative Controls and Procedures	Additional Considerations
4.0	**The entity collects personal information only for the purposes identified in the notice.**		
4.1	**Policies and Communications**		
4.1.0	**Privacy Policies** The entity's privacy policies address the collection of personal information.		Some jurisdictions, such as some countries in Europe, require entities that collect personal information to register with their regulatory body.
4.1.1	**Communication to Individuals** Individuals are informed that personal information is collected only for the purposes identified in the notice.	The entity's privacy notice discloses the types of personal information collected, the sources and methods used to collect personal information, and whether information is developed or acquired about individuals, such as buying patterns.	
4.1.2	**Types of Personal Information Collected and Methods of Collection** The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Types of personal information collected include the following: • Financial (for example, financial account information) • Health (for example, information about physical or mental status or history) • Demographic (for example, age, income range, social geocodes) Methods of collecting and third-party sources of personal information include the following: • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons The entity's privacy notice discloses whether it uses cookies and Web	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

Ref.	Collection Criteria	Illustrative Controls and Procedures	Additional Considerations
		beacons and how they are used. The notice also describes the consequences if the cookie is refused.	
4.2	**Procedures and Controls**		
4.2.1	**Collection Limited to Identified Purpose** The collection of personal information is limited to that necessary for the purposes identified in the notice.	Systems and procedures are in place to • 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 changes to the program or service are made). • 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.	

Ref.	Collection Criteria	Illustrative Controls and Procedures	Additional Considerations
4.2.2	**Collection by Fair and Lawful Means** Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (*a*) fairly, without intimidation or deception, and (*b*) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	The entity's management, privacy officer, and legal counsel, review the methods of collection and any changes thereto.	The following may be considered deceptive practices: • 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 • To use a third party to collect information in order to avoid providing notice to individuals Entities should consider legal and regulatory requirements in jurisdictions other than the one in which they operate (for example, an entity in Canada collecting personal information about Europeans may be subject to certain European legal requirements). A review of complaints may help to identify whether unfair or unlawful practices exist.
4.2.3	**Collection From Third Parties** Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	The entity • performs due diligence before establishing a relationship with a third-party data provider. • reviews the privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources.	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources.

Ref.	Collection Criteria	Illustrative Controls and Procedures	Additional Considerations
4.2.4	**Information Developed about Individuals** Individuals are informed if the entity develops or acquires additional information about them for its use.	The entity's privacy notice indicates that, if applicable, it may develop and acquire information about the individual using third-party sources, browsing, credit and purchasing history, and so on.	

Use, Retention, and Disposal

Ref.	Use, Retention, and Disposal Criteria	Illustrative Controls and Procedures	Additional Considerations
5.0	**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 or as required by law or regulations and thereafter appropriately disposes of such information.**		
5.1	**Policies and Communications**		
5.1.0	**Privacy Policies** The entity's privacy policies address the use, retention, and disposal of personal information.		
5.1.1	**Communication to Individuals** Individuals are informed that personal information is (*a*) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (*b*) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (*c*) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.	The entity's privacy notice describes the following uses of personal information, for example: • Processing business transactions such as claims and warranties, payroll, taxes, benefits, stock options, bonuses, or other compensation schemes • Addressing inquiries or complaints about products or services, or interacting during the promotion of products or services • Product design and development, or purchasing of products or services • Participation in scientific or medical research activities, marketing, surveys, or market analysis • Personalization of Web sites or downloading software • Legal requirements • Direct marketing	

Ref.	Use, Retention, and Disposal Criteria	Illustrative Controls and Procedures	Additional Considerations
		The entity's privacy notice explains that personal information will be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and thereafter will be disposed of securely or made anonymous so that it cannot be identified to any individual.	
5.2	**Procedures and Controls**		
5.2.1	**Use of Personal Information** Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	Systems and procedures are in place to ensure that personal information is used • in conformity with the purposes identified in the entity's privacy notice. • in agreement with the consent received from the individual. • in compliance with applicable laws and regulations.	Some regulations have specific provisions concerning the use of personal information. Examples are the GLBA, the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).
5.2.2	**Retention of Personal Information** Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.	The entity • documents its retention policies and disposal procedures. • retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies. • ensures personal information is not kept beyond the standard retention time unless a justified business or legal reason for doing so exists. Contractual requirements are considered when establishing retention practices when they may be	Some laws specify the retention period for personal information. For example, HIPAA has retention requirements on accounting for disclosures of personal health information—three years for electronic health records, and six years for nonelectronic health records. Other statutory record retention requirements may exist; for example, certain data may need to be retained for tax purposes or in accordance with employment laws.

Ref.	Use, Retention, and Disposal Criteria	Illustrative Controls and Procedures	Additional Considerations
		exceptions to normal policies.	
5.2.3	**Disposal, Destruction and Redaction of Personal Information** Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	The entity • erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). • disposes of original, archived, backup and ad hoc or personal copies of records in accordance with its destruction policies. • documents the disposal of personal information. • within the limits of technology, locates and removes or redacts specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete. • regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or as required by laws and regulations. Contractual requirements are considered when establishing disposal, destruction, and redaction practices if they may result in exception to the entity's normal policies.	Consideration should be given to using the services of companies that provide secure destruction services for personal information. Certain of these companies will provide a certificate of destruction where needed. Certain archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without destruction of the entire database contained on such media.

Access

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
6.0	**The entity provides individuals with access to their personal information for review and update.**		
6.1	**Policies and Communications**		
6.1.0	**Privacy Policies** The entity's privacy policies address providing individuals with access to their personal information.		
6.1.1	**Communication to Individuals** Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.	The entity's privacy notice • explains how individuals may gain access to their personal information and any costs associated with obtaining such access. • outlines the means by which individuals may update and correct their personal information (for example, in writing, by phone, by e-mail, or by using the entity's Web site). • explains how disagreements related to personal information may be resolved.	
6.2	**Procedures and Controls**		
6.2.1	**Access by Individuals to Their Personal Information** Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	Procedures are in place to • determine whether the entity holds or controls personal information about an individual. • communicate the steps to be taken to gain access to the personal information. • respond to an individual's request on a timely basis. • provide a copy of personal	Some laws and regulations specify the following: • Provisions and requirements for providing access to personal information (for example, HIPAA) • Requirements that requests for access to personal information be submitted in writing

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
		information, upon request, in printed or electronic form that is convenient to both the individual and the entity. • record requests for access and actions taken, including denial of access and unresolved complaints and disputes.	
6.2.2	**Confirmation of an Individual's Identity** The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	Employees are adequately trained to authenticate the identity of individuals before granting the following: • Access to their personal information • Requests to change sensitive or other personal information (for example, to update information such as address or bank details) The entity • does not use government-issued identifiers (for example, Social Security numbers or Social Insurance numbers) for authentication. • mails information about a change request only to the address of record or, in the case of a change of address, to both the old and new addresses. • requires that a unique user identification and password (or equivalent) be used to access user account information online.	The extent of authentication depends on the type and sensitivity of personal information that is made available. Different techniques may be considered for the different channels, such as the following: • Web • Interactive voice response system • Call center • In person
6.2.3	**Understandable Personal Information, Time Frame, and Cost**	The entity • provides personal information to the individual in a format that is	Entities may provide individuals with access to their personal information at no cost or at a minimal cost

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
	Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	understandable (for example, not in code, not in a series of numbers, not in overly technical language or other jargon), and in a form convenient to both the individual and the entity. • makes a reasonable effort to locate the personal information requested and, if personal information cannot be found, keeps sufficient records to demonstrate that a reasonable search was made. • takes reasonable precautions to ensure that personal information released does not identify another person, directly or indirectly. • provides access to personal information in a timeframe that is similar to the entity's normal response times for other business transactions, or as permitted or required by law. • provides access to personal information in archived or backup systems and media. • informs individuals of the cost of access at the time the access request is made or as soon as practicable thereafter. • charges the individual for access to personal information at an amount, if any, which is not excessive in relation to the entity's cost of providing access. • provides an appropriate physical space to inspect personal information.	because of the potential business and customer-relationship benefits, as well as the opportunity to enhance the quality of the information.

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
6.2.4	**Denial of Access** Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	The entity • outlines the reasons why access to personal information may be denied. • records all denials of access and unresolved complaints and disputes. • provides the individual with partial access in situations in which access to some of his or her personal information is justifiably denied. • provides the individual with a written explanation about why access to personal information is denied. • provides a formal escalation (appeal) process if access to personal information is denied. • conveys the entity's legal rights and the individual's right to challenge, if applicable.	Some laws and regulations (for example, Principle 5, "Information relating to records kept by record-keeper," point 2 of the Australian Privacy Act of 1988, and PIPEDA, Sections 8.(4), 8.(5), 8.(7), 9, 10, and 28) specify the situations in which access can be denied, the process to be followed (such as notifying the customer of the denial in writing within 30 days), and potential penalties or sanctions for lack of compliance.
6.2.5	**Updating or Correcting Personal Information** Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	The entity • describes the process an individual must follow to update or correct personal information records (for example, in writing, by phone, by e-mail, or by using the entity's Web site). • verifies the accuracy and completeness of personal information that an individual updates or changes (for example, by edit and validation controls, and forced completion of mandatory fields).	In some jurisdictions (for example, PIPEDA, Schedule 1, clauses 4.5.2 and 4.5.3), personal information cannot be erased, but an entity is bound to cease further processing.

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
		• records the date, time, and identification of the person making the change if the entity's employee is making a change on behalf of an individual. • notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so.	
6.2.6	**Statement of Disagreement** Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask the entity to accept a statement claiming that the personal information is not complete and accurate. The entity • documents instances where an individual and the entity disagree about whether personal information is complete and accurate. • informs the individual, in writing, of the reason a request for correction of personal information is denied, citing the individual's right to appeal. • informs the individual, when access to personal information is requested or when access is actually provided, that the statement of disagreement may include information about the nature of the change sought by the individual and the reason for	See 10.1.1, "Communications to Individuals," 10.2.1, "Inquiry, Complaint, and Dispute Process," and 10.2.2, "Dispute Resolution and Recourse." Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of disagreements from individuals. If a challenge is not resolved to the satisfaction of the individual, when appropriate, the existence of such challenge is communicated to third parties having access to the information in question.

Ref.	Access Criteria	Illustrative Controls and Procedures	Additional Considerations
		its refusal by the entity. • if appropriate, notifies third parties who have previously been provided with personal information that there is a disagreement and the nature of the disagreement.	

Disclosure to Third Parties

Ref.	Disclosure to Third Parties Criteria	Illustrative Controls and Procedures	Additional Considerations
7.0	**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.**		
7.1	**Policies and Communications**		
7.1.0	**Privacy Policies** The entity's privacy policies address the disclosure of personal information to third parties.		
7.1.1	**Communication to Individuals** Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.	The entity's privacy notice • describes the practices related to the sharing of personal information (if any) with third parties and the reasons for information sharing. • identifies third parties or classes of third parties to whom personal information is disclosed. • informs individuals that personal information is disclosed to third parties only for the purposes (*a*) identified in the notice, and (*b*) for which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation.	The entity's privacy notice may disclose the following: • The process used to assure the privacy and security of personal information that has been disclosed to a third party • How personal information shared with a third party will be kept up to date, so that outdated or incorrect information shared with a third party will be changed if the individual has changed his or her information
7.1.2	**Communication to Third Parties** Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.	Prior to sharing personal information with a third party, the entity communicates its privacy policies or other specific instructions or requirements for handling personal information to, and obtains a written agreement from the third party that its privacy practices over the	

Ref.	Disclosure to Third Parties Criteria	Illustrative Controls and Procedures	Additional Considerations
		disclosed personal information adhere to those policies or requirements.	
7.2	**Procedures and Controls**		
7.2.1	**Disclosure of Personal Information** Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.	Systems and procedures are in place to • prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure. • document the nature and extent of personal information disclosed to third parties. • test whether disclosure to third parties is in compliance with the entity's privacy policies and procedures, or as specifically allowed or required by law or regulation. • document any third-party disclosures for legal reasons.	Personal information may be disclosed through various legal processes to law enforcement or regulatory agencies. Some laws and regulations have specific provisions for the disclosure of personal information. Some permit disclosure of personal information without consent whereas others require verifiable consent.
7.2.2	**Protection of Personal Information** Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	When providing personal information to third parties, the entity enters into contracts that require a level of protection of personal information equivalent to that of the entity's. In doing so, the entity • limits the third party's use of personal information to purposes necessary to fulfill the contract. • communicates the individual's preferences to the third party. • refers any requests for access or complaints about the personal information transferred by the entity to a designated privacy	The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party. Some regulations (for example, from the U.S. federal financial regulatory agencies) require that an entity take reasonable steps to oversee appropriate service providers by exercising appropriate due diligence in the selection of service providers. Some jurisdictions, including some

Ref.	Disclosure to Third Parties Criteria	Illustrative Controls and Procedures	Additional Considerations
		executive, such as a corporate privacy officer. • specifies how and when third parties are to dispose of or return any personal information provided by the entity. The entity evaluates compliance with such contract using one or more of the following approaches to obtain an increasing level of assurance depending on its risk assessment: • The third party responds to a questionnaire about their practices. • The third party self-certifies that its practices meet the entity's requirements based on internal audit reports or other procedures. • The entity performs an onsite evaluation of the third party. • The entity receives an audit or similar report provided by an independent auditor.	countries in Europe, require entities that transfer personal information to register with their regulatory body prior to transfer. PIPEDA requires a comparable level of protection while the personal information is being processed by a third party. Article 25 of the EU's Directive requires that such transfers take place only where the third party ensures an adequate level of protection.
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Systems and procedures are in place to • notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice. • document whether the entity has notified the individual and received the individual's consent. • monitor that personal information is being provided to third parties only for uses	Other types of onward transfers include transfers to third parties who are • subsidiaries or affiliates. • providing a service requested by the individual. • law enforcement or regulatory agencies. • in another country and may be subject to other requirements.

Ref.	Disclosure to Third Parties Criteria	Illustrative Controls and Procedures	Additional Considerations
		specified in the privacy notice.	
7.2.4	**Misuse of Personal Information by a Third Party** The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The entity • reviews complaints to identify indications of any misuse of personal information by third parties. • responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements. • 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 affected numbers and reissue new numbers). • takes remedial action in the event that a third party misuses personal information (for example, contractual clauses address the ramification of misuse of personal information).	

Security for Privacy

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
8.0	**The entity protects personal information against unauthorized access (both physical and logical).**		
8.1	**Policies and Communications**		
8.1.0	**Privacy Policies** The entity's privacy policies (including any relevant security policies), address the security of personal information.	Privacy policies adequately address security measures to safeguard the privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal information.	Personal information in any location under control of the entity or deemed to be under control of the entity must be protected.
8.1.1	**Communication to Individuals** Individuals are informed that precautions are taken to protect personal information.	The entity's privacy notice describes the general types of security measures used to protect the individual's personal information, for example: • Employees are authorized to access personal information based on job responsibilities. • Authentication is used to prevent unauthorized access to personal information stored electronically. • Physical security is maintained over personal information stored in hard copy form, and encryption is used to prevent unauthorized access to personal information sent over the Internet. • Additional security safeguards are applied to sensitive information.	Users, management, providers, and other parties should strive to develop and adopt good privacy practices and to promote conduct that recognizes security needs and respects the legitimate interests of others. Consideration should be given to disclosing in the privacy notice the security obligations of individuals, such as keeping user IDs and passwords confidential and reporting security compromises. Consideration should be given to limiting the disclosure of detailed security procedures so as not to compromise internal security.
8.2	**Procedures and Controls**		

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
8.2.1	**Information Security Program** A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas[3] insofar as they relate to the security of personal information: *a.* Risk assessment and treatment [1.2.4] *b.* Security policy [8.1.0] *c.* Organization of information security [sections 1, 7, and 10] *d.* Asset management [section 1] *e.* Human resources security [section 1] *f.* Physical and environmental security [8.2.3 and 8.2.4] *g.* Communications and operations management [sections 1, 7, and 10] *h.* Access control [sections 1, 8.2, and 10] *i.* Information systems acquisition, development, and maintenance [1.2.6]	The entity's security program addresses the following matters related to protection of personal information: • Periodic risk assessments • Identification of all types of personal information and the related processes, systems, and third parties that are involved in the handling of such information • Identification and documentation of the security requirements of authorized users • Allowing access, the nature of that access, and who authorizes such access • Preventing unauthorized access by using effective physical and logical access controls • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Assignment of responsibility and accountability for security • Assignment of responsibility and accountability for system changes and maintenance • Protecting operating system and network software and system files	Safeguards employed may consider the nature and sensitivity of the data, as well as the size and complexity of the entity's operations. For example, the entity may protect personal information and other sensitive information to a level greater than it applies for other information. Some regulations (for example, HIPAA) provide a greater level of detail and guidance on specific security measures to be considered and implemented. Some security rules (for example, GLBA-related rules for safeguarding information) require the following: • Board (or committee or individual appointed by the board) approval and oversight of the entity's information security program. • That an entity take reasonable steps to oversee appropriate service providers by – exercising appropriate due diligence in the selection of service providers. – requiring service providers by contract to implement and maintain

3 These areas are drawn from ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at http://webstore.ansi.org/ and in Canada from the Standards Council of Canada at www.standardsstore.ca/eSpecs/index.jsp. It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy *Generally Accepted Privacy Principles*' criterion 8.2.1. The references associated with each area indicate the most relevant *Generally Accepted Privacy Principles*' criteria for this purpose.

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
	j. Information security incident management [1.2.7] *k.* Business continuity management [section 8.2] *l.* Compliance [sections 1 and 10]	• Protecting cryptographic tools and information • Implementing system software upgrades and patches • Testing, evaluating, and authorizing system components before implementation • Addressing how complaints and requests relating to security issues are resolved • Handling errors and omissions, security breaches, and other incidents • Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing) • Allocating training and other resources to support its security policies • Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies • Business continuity management and disaster recovery plans and related testing • Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts • A requirement that users, management, and third parties	appropriate safeguards for the personal information at issue. The payment card industry has established specific security and privacy requirements for cardholder information from certain brands.

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
		confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information • Procedures to cancel access privileges and ensure return of computers and other devices used to access or store personal information when personnel are terminated The entity's security program prevents access to personal information in computers, media, and paper based information that are no longer in active use by the organization (for example, computers, media, and paper-based information in storage, sold, or otherwise disposed of).	
8.2.2	**Logical Access Controls** Logical access to personal information is restricted by procedures that address the following matters: *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 privileges and permissions for access to IT	Systems and procedures are in place to • establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information. • authenticate users, for example, by user name and password, certificate, external token, or biometrics before access is granted to systems handling personal information. • require enhanced security	User authorization processes consider the following: • How the data is accessed (internal or external network), as well as the media and technology platform of storage • Access to paper and backup media containing personal information • Denial of access to joint accounts without other methods to authenticate the actual individuals Some jurisdictions require stored data

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
	infrastructure components and personal information *e.* Preventing individuals from accessing anything 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) *j.* Preventing the introduction of viruses, malicious code, and unauthorized software	measures for remote access, such as additional or dynamic passwords, callback procedures, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls. • implement intrusion detection and monitoring systems.	(at rest) to be encrypted or otherwise obfuscated.
8.2.3	**Physical Access Controls** Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Systems and procedures are in place to • manage logical and physical access to personal information, including hard copy, archival, and backup copies. • log and monitor access to personal information. • prevent the unauthorized or accidental destruction or loss of personal information. • investigate breaches and	Physical safeguards may include the use of locked file cabinets, card access systems, physical keys, sign in logs, and other techniques to control access to offices, data centers, and other locations in which personal information is processed or stored.

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
		attempts to gain unauthorized access. • communicate investigation results to the appropriate designated privacy executive. • maintain physical control over the distribution of reports containing personal information. • securely dispose of waste containing confidential information (for example, shredding).	
8.2.4	**Environmental Safeguards** Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. In addition, the entity maintains physical and other safeguards to prevent accidental disclosure of personal information in the event of an environmental incident.	Some regulations, such as those in the EU Directive, also require that personal information is protected against unlawful destruction, accidental loss, natural disasters, and environmental hazards, in addition to accidental disclosure.
8.2.5	**Transmitted Personal Information** Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying	Systems and procedures are in place to • define minimum levels of encryption and controls. • employ industry standard encryption technology, for example, 128-bit Transport Layer Security (TLS), over VPNs,	Some regulations (for example, HIPAA) have specific provisions for the electronic transmission and authentication of signatures with respect to health information records (that is, associated with the standard transactions).

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
	industry standard encryption technology for transferring and receiving personal information.	for transferring and receiving personal information. • approve external network connections. • protect personal information in both hardcopy and electronic forms sent by mail, courier, or other physical means. • encrypt personal information collected and transmitted wirelessly and protect wireless networks from unauthorized access.	Some credit card vendors have issued minimum requirements for protecting cardholder data, including the requirement to use encryption techniques for credit card and transaction related data in transmission and in storage. As technology, market, and regulatory conditions evolve, new measures may become necessary to meet acceptable levels of protection (for example, 128-bit secure TLS, including user IDs and passwords). Voice transmission from wireless devices (for example, cell phones) of personal information may not be encrypted.
8.2.6	**Personal Information on Portable Media** Personal information stored on portable media or devices is protected from unauthorized access.	Policies and procedures prohibit the storage of personal information on portable media or devices unless a business need exists and such storage is approved by management. Policies, systems, and procedures are in place to protect personal information accessed or stored in manners such as using the following: • Laptop computers, PDAs, smart-phones and similar devices • Computers and other devices used by employees while, for example, traveling and working at home • USB drives, CDs and DVDs, magnetic tape, or other portable media	Consideration should be given to the protection needed for any personal information provided to, for example, regulators and auditors.

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
		Such information is encrypted, password protected, physically protected, and subject to the entity's access, retention, and destruction policies. Controls exist over creation, transfer, storage, and disposal of media containing personal information used for backup and recovery. Procedures exist to report loss or potential misuse of media containing personal information. Upon termination of employees or contractors, procedures provide for the return or destruction of portable media and devices used to access and store personal information, and of printed and other copies of such information.	
8.2.7	**Testing Security Safeguards** Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Systems and procedures are in place to • regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information. • periodically undertake independent audits of security controls using either internal or external auditors. • test card access systems and other physical security devices at least annually. • document and test disaster recovery and contingency plans	The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to • conduct regular tests of key controls, systems, and procedures by independent third parties or by staff independent of

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
		at least annually to ensure their viability. • periodically undertake threat and vulnerability testing, including security penetration and Web vulnerability and resilience. • 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. • periodically report the results of security testing to management.	those that develop or maintain security (or at least have these independent parties review results of testing). • assess and possibly adjust its information security at least annually.

Quality

Ref.	Quality Criteria	Illustrative Controls and Procedures	Additional Consideration
9.0	**The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.**		
9.1	**Policies and Communications**		
9.1.0	**Privacy Policies** The entity's privacy policies address the quality of personal information.		
9.1.1	**Communication to Individuals** Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.	The entity's privacy notice explains that personal information needs to be kept accurate and complete only when the individual has an ongoing relationship with the entity.	
9.2	**Procedures and Controls**		
9.2.1	**Accuracy and Completeness of Personal Information** Personal information is accurate and complete for the purposes for which it is to be used.	Systems and procedures are in place to • edit and validate personal information as it is collected, created, maintained, and updated. • record the date when the personal information is obtained or updated. • specify when the personal information is no longer valid. • 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	

Ref.	Quality Criteria	Illustrative Controls and Procedures	Additional Consideration
		information). • indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, received from a third party (see 4.2.3, "Collection From Third Parties"), or disclosed to a third party (see 7.2.2, "Protection of Personal Information"). • ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless clear limits exist for the need for accuracy. • ensure personal information is not routinely updated unless such a process is necessary to fulfill the purposes for which it is to be used. The entity undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary, to fulfill the stated purpose.	
9.2.2	**Relevance of Personal Information** Personal information is relevant to the purposes for which it is to be used.	Systems and procedures are in place to • ensure personal information is sufficiently relevant for the purposes for which it is to be used and to minimize the possibility that inappropriate information is used to make business decisions about the individual.	

Ref.	Quality Criteria	Illustrative Controls and Procedures	Additional Consideration
		• periodically assess the relevance of personal information records and to correct them, as necessary, to minimize the use of inappropriate data for decision making.	

Monitoring and Enforcement

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
10.0	**The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.**		
10.1	**Policies and Communications**		
10.1.0	**Privacy Policies** The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.		
10.1.1	**Communication to Individuals** Individuals are informed about how to contact the entity with inquiries, complaints and disputes.	The entity's privacy notice • describes how individuals can contact the entity with complaints (for example, via an e-mail link to the entity's Web site or a telephone number). • provides relevant contact information to which the individual can direct complaints (for example, name, telephone number, mailing address, and e-mail address of the individual or office responsible for handling complaints).	
10.2	**Procedures and Controls**		
10.2.1	**Inquiry, Complaint, and Dispute Process** A process is in place to address inquiries, complaints, and disputes.	The corporate privacy officer or other designated individual is authorized to address privacy related complaints, disputes, and other problems. Systems and procedures are in place that allow for • procedures to be followed in communicating and resolving complaints about the entity.	

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
		• action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved. • remedies to be available in case of a breach of personal information and how to communicate this information to an individual. • recourse and a formal escalation process to be in place to review and approve any recourse offered to individuals. • contact information and procedures to be followed with any designated third party dispute resolution or similar service (if offered).	
10.2.2	**Dispute Resolution and Recourse** Each complaint is addressed, and the resolution is documented and communicated to the individual.	The entity has a formally documented process in place to • train employees responsible for handling individuals' complaints and disputes about the resolution and escalation processes. • document and respond to all complaints in a timely manner. • periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner. • escalate unresolved complaints and disputes for review by management. • identify trends and the potential need to change the entity's privacy policies and procedures. • use specified independent third-	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements. Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
		party dispute resolution services or other processes mandated by regulatory bodies in the event the individual is not satisfied with the entity's proposed resolution, together with a commitment from such third parties to handle such recourses. If the entity offers a third-party dispute resolution process for complaints that cannot be resolved directly with the entity, an explanation is provided about how an individual can use that process.	
10.2.3	**Compliance Review** Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Systems and procedures are in place to • annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, standards adopted by the entity, and other contracts. • document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign offs. • report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan. • monitor the resolution of issues and vulnerabilities noted in the	In addition to legal, regulatory and contractual requirements, some entities may elect to comply with certain standards, such as those published by ISO, or may be required to comply with certain standards, such as those published by the payment card industry, as a condition of doing business.

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
		compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary).	
10.2.4	**Instances of Noncompliance** Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Systems and procedures are in place to • notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner. • inform employees of the appropriate channels to report security vulnerabilities and privacy breaches. • document instances of noncompliance with privacy policies and procedures. • monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis. • discipline employees and others, as appropriate, who cause privacy incidents or breaches. • mitigate, 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 affected account numbers and reissue new numbers).	

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
		• identify trends that may require revisions to privacy policies and procedures.	
10.2.5	**Ongoing Monitoring** Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary.	The entity uses the following: • Control reports • Trend analysis • Training attendance and evaluations • Complaint resolutions • Regular internal reviews • Internal audit reports • Independent audit reports covering controls at service organizations • Other evidence of control effectiveness The selection of controls to be monitored, and the frequency with which they are monitored are based on the sensitivity of the information and the risks of possible exposure of the information. Examples of such controls are as follows: • Policies require that all employees take initial privacy training within 30 days of employment. Ongoing monitoring activities would include a review of human resource files of selected employees to determine that they contain the appropriate evidence of course completion.	*Guidance on Monitoring Internal Control Systems*, published by COSO (the Committee of Sponsoring Organizations of the Treadway Commission), provides helpful guidance for monitoring the effectiveness of controls.

Ref.	Monitoring and Enforcement Criteria	Illustrative Controls and Procedures	Additional Considerations
		• Policies require that whenever an employee changes job responsibilities or is terminated, such employee's access to personal information be reviewed and appropriately modified or terminated within 24 hours (or immediately in the case of employee termination). This is controlled by an automated process within the human resource system which produces a report of employee status changes, which requires supervisor action to avoid automatic termination of access. This is monitored by the security group which receives copies of these reports and the related supervisor actions. • Policies state that confirmation of a privacy-related complaint is provided to the complainant within 72 hours, and if not resolved within 10 working days, then the issue is escalated to the CPO. The control is a log used to record privacy complaints, including complaint date, and subsequent activities through to resolution. The monitoring activity is the monthly review of such logs for consistency with this policy.	

Appendix A—Glossary

affiliate. An entity that controls, is controlled by, or is under common control with another entity.

anonymize. The removal of any person-related information that could be used to identify a specific individual.

confidentiality. The protection of nonpersonal information and data from unauthorized disclosure.

consent. Agreement by the individual for the entity to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. *Explicit consent* is given orally, electronically, or in writing, is unequivocal and does not require any inference on the part of the entity seeking consent. *Implicit consent* may reasonably be inferred from the action or inaction of the individual such as not having *opted out*, or providing credit card information to complete a transaction. (see opt in and opt out).

cookies. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. The information can then be used to identify the user when returning to the Web site, to personalize Web content, and suggest items of potential interest based on previous buying habits. Certain advertisers use tracking methods, including cookies, to analyze the patterns and paths through a site.

encryption. The process of transforming information to make it unreadable to anyone except those possessing special key (to decrypt).

entity. An organization that collects, uses, retains, and discloses personal information.

individual. The person about whom the personal information is being collected (sometimes referred to as the *data subject*).

internal personnel. Employees, contractors, agents, and others acting on behalf of the entity and its affiliates.

opt in. Personal information may not be collected, used, retained and disclosed by the entity without the explicit consent of the individual.

opt out. Implied consent exists for the entity to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

outsourcing. The use and handling of personal information by a third party that performs a business function for the entity.

personal information. Information that is or can be about or related to an identifiable individual.

personal information cycle. The collection, use, retention, disclosure, disposal, or anonymization of personal information.

policy. A written statement that communicates management's intent, objectives, requirements, responsibilities, and standards.

privacy. The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.

privacy breach. 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.

privacy program. The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with business and compliance risks and requirements.

purpose. The reason personal information is collected by the entity.

redact. To delete or black out personal information from a document or file.

sensitive personal information. Personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

third party. An entity that is not affiliated with the entity that collects personal information or any affiliated entity not covered by the entity's privacy notice.

Web beacon. Web beacons, also known as Web bugs, are small strings of code that provide a method for delivering a graphic image on a Web page or in an e-mail message for the purpose of transferring data. Businesses use Web beacons for many purposes, including site traffic reporting, unique visitor counts, advertising and e-mail auditing and reporting, and personalization. For example, a Web beacon can gather a user's IP address, collect the referrer, and track the sites visited by users.

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA

barcode here