

Generally Accepted Privacy Principles

A Global Privacy Framework

May 2006





Acknowledgments:

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

- ISACA



- The Institute of Internal Auditors



*Copyright © 2006 by
American Institute of Certified Public Accountants, Inc. and Canadian Institute of
Chartered Accountants.*

*All rights reserved. Checklists and sample documents contained herein may be
reproduced and distributed as part of professional services or within the context of
professional practice, provided that reproduced materials are not in any way
directly offered for sale or profit. For information about the procedure for
requesting permission to make copies of any part of this work, please visit
www.copyright.com or call (978) 750-8400.*

Foreword

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) believe strongly that privacy is a business issue. In 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 contribute significantly by developing a privacy framework that would address the needs and expectations of all of the parties affected by privacy requirements or expectations. Therefore, the institutes developed the initial AICPA/CICA Privacy Framework. This framework has been updated to reflect that the principles included have now become more widely accepted. Accordingly, the framework has now been renamed as 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 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.

Underlying these principles is the premise 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. Since more data is 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 even a more significant challenge. Organizations need to be aware of the significant privacy requirements in all the jurisdictions in which the organization does business.

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 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 examination (which is usually referred to as a “privacy audit”) can be performed.

Generally Accepted Privacy Principles represent the AICPA and CICA contribution to the effective management of privacy risk, recognizing the needs of organizations while reflecting the public interest. Additional history about the development and additional privacy resources can be found at www.aicpa.org/privacy and www.cica.ca/privacy. *Generally Accepted Privacy Principles - A Global Privacy Framework* can be downloaded from the [AICPA](#) and the [CICA](#) Web sites.*

The development and maintenance of Generally Accepted Privacy Principles is a dynamic process; as a result, please forward any comments about this document to the AICPA (ncohen@aicpa.org) or the CICA (privacy@cica.ca).

AICPA

CICA

May 2006

* The respective URLs are <http://infotech.aicpa.org/Resources/Privacy/> and http://www.cica.ca/index.cfm/ci_id/258/la_id/1.htm.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA
Deloitte & Touche LLP (retired)

Vice Chair

Kenneth D. Askelson,
CPA/CITP, CIA

Eric Federling
KPMG LLP

Don H. Hansen, CPA
Moss Adams LLP

Philip M. Juravel, CPA
Juravel & Company, LLC

Sagi Leizerov, Ph.D.
Ernst & Young LLP

Marilyn Prosch, Ph.D.
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
Deloitte & Touche LLP

Staff Contact:

Bryan Walker, CA, CICA
*Principal, Assurance Services
Development*

Nancy A. Cohen, CPA
*Senior Technical Manager,
InfoTechnology Communities*

Generally Accepted Privacy Principles –
A Global Privacy Framework was
approved by the AICPA Board of
Directors.

Table of Contents

PRIVACY – AN INTRODUCTION TO GENERALLY ACCEPTED PRIVACY PRINCIPLES	1
INTRODUCTION	1
<i>Why Privacy Is a Business Issue</i>	1
INTERNATIONAL PRIVACY CONSIDERATIONS	2
<i>Outsourcing and Privacy</i>	3
WHAT IS PRIVACY?	4
<i>Privacy Definition</i>	4
<i>Personal Information</i>	4
<i>Privacy or Confidentiality?</i>	5
INTRODUCING GENERALLY ACCEPTED PRIVACY PRINCIPLES	6
OVERALL PRIVACY OBJECTIVE	6
GENERALLY ACCEPTED PRIVACY PRINCIPLES	6
<i>Using Generally Accepted Privacy Principles</i>	8
<i>Presentation of Generally Accepted Privacy Principles and Criteria</i>	11
GENERALLY ACCEPTED PRIVACY PRINCIPLES AND CRITERIA	12
MANAGEMENT	12
NOTICE	18
CHOICE AND CONSENT	22
COLLECTION	27
USE AND RETENTION	30
ACCESS	33
DISCLOSURE TO THIRD PARTIES	39
SECURITY FOR PRIVACY	43
QUALITY	50
MONITORING AND ENFORCEMENT	53
APPENDIX A - GLOSSARY	57
APPENDIX B - COMPARISON OF INTERNATIONAL PRIVACY CONCEPTS	60

Privacy – An Introduction to Generally Accepted Privacy Principles

Introduction

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

Generally Accepted Privacy Principles have been developed from a business perspective, referencing significant domestic and international privacy regulations. Generally Accepted Privacy Principles operationalize complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that need to be met. Illustrative policy requirements, communications, and controls, including monitoring controls, are provided as support for the criteria.

This document sets out Generally Accepted Privacy Principles that can be used by any organization as part of its [privacy program](#). Generally Accepted Privacy Principles have been developed to help management create an effective privacy program that addresses privacy risks and obligations and business opportunities. 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 the organizations and their customers.

This introduction and the set of Generally Accepted Privacy Principles and Criteria 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
- Assess compliance and audit privacy and security programs
- Regulate privacy

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

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 Criteria tables.

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 but, 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. Specific risks of having inadequate privacy policies and procedures include:

- 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

International Privacy Considerations

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

For example, the global nature of the Internet and business means that regulatory actions in one country may affect the rights and obligations of users around the world. Many countries have laws regulating transborder

data flow, including the European Union's 1995 and 1997 directives on data protection and privacy with which an organization must comply if it wants to do business in those jurisdictions. 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 in trying to 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 emerging regulations will be facilitated.

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

Outsourcing and Privacy

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

The Generally Accepted Privacy Principles and supporting Criteria set out in this document can assist an organization in completing assessments (including independent examinations) about the privacy policies, procedures, and practices of the entity performing the outsourcing to which part of its privacy responsibility has been transferred.

The fact that these principles 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 included in many privacy laws and regulations of various jurisdictions around the world and recognized as good privacy practices.

What Is Privacy?

Privacy Definition

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

Personal Information

Personal information is information that is, or can be, about or 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. 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:

- Name
- Home or e-mail address
- Identification number (e.g., 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, the use of sensitive information may require explicit consent rather than implicit consent.

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 “de-identified” or “anonymized.” Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual.

Privacy or Confidentiality?

Unlike personally identifiable information, which is often defined by regulation in a number of countries worldwide, there is no single definition of confidential information 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 to be maintained on a “need to know” basis. Examples of the kinds of information that may be subject to a [confidentiality](#) requirement include:

- 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. The AICPA/CICA Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (including WebTrust® and SysTrust®) provides a set of criteria for confidentiality (see www.webtrust.org).

Introducing Generally Accepted Privacy Principles

Generally Accepted Privacy Principles are designed to assist management in creating an effective privacy program that addresses their privacy risks and business opportunities.

The set of Generally Accepted Privacy Principles is founded on key concepts from significant domestic and international privacy laws, regulations, and guidelines (see Appendix B, “Comparison of International Privacy Concepts”)² and good business practices. By using these Generally Accepted Privacy Principles, organizations can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. The use of Generally Accepted Privacy Principles also facilitates management of privacy risk on a multijurisdictional basis.

Overall Privacy Objective

Generally Accepted Privacy Principles are founded on the following privacy objective.

Personal information is collected, used, retained, and disclosed 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/CICA.

Generally Accepted Privacy Principles

Generally Accepted Privacy Principles are essential to the proper protection and management of personal information. They are based on internationally

² For example, the Organisation for Economic Co-operation and Development (OECD) has issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) and the European Union (EU) has issued Directive on Data Privacy (Directive 95/46/EC). In addition, the United States has enacted the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children’s Online Privacy Protection Act (COPPA). Canada has enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) and Australia has enacted the Australian Privacy Act of 1988, as amended in 2001. Web site URLs for these and other privacy laws and regulations are set out in Appendix B. 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 may wish to seek appropriate legal advice regarding compliance with any laws and regulations.

known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

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 and Retention](#). 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.
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 developed for evaluating an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and/or 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 Generally Accepted Privacy Principles

Generally Accepted Privacy Principles can be used by organizations for:

- Privacy [policy](#) design and implementation
- Performance measurement
- Benchmarking
- Monitoring and auditing privacy programs

Management of a privacy program entails the following activities:

- Strategizing—Performing privacy strategic and business planning
- Diagnosing—Performing privacy gap and risk analysis
- Implementing—Introducing and institutionalizing solutions
- Sustaining/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 Generally Accepted Privacy Principles can be used by an organization to address these business activities.

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
Strategizing	<p>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.</p> <p>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 and major issues for becoming privacy-compliant.</p>	<p>Vision. Within an entity’s privacy effort, establishing the vision helps the entity integrate preferences and prioritize goals.</p> <p>Strategic Planning. Within an entity’s privacy effort, Generally Accepted Privacy Principles can be used to assist the organization in identifying significant components that need to be addressed.</p>

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	<p>Resource Allocation. This step identifies the human and financial resources allocated to achieve the goals and objectives set forth in the strategic plan or business plan.</p>	<p>Resource Allocation. Using Generally Accepted Privacy Principles, the entity would identify the people working with and responsible for areas that might include systems management, privacy and security concerns, and stipulate the budget for their activities.</p> <p>Overall Strategy. A strategic document describes expected or intended future development. Generally Accepted Privacy Principles 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.</p>
Diagnosing	<p>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 engagement for an organization is an assessment. The purpose of 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.</p>	<p>Generally Accepted Privacy Principles 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.</p> <p>Generally Accepted Privacy Principles provides a legislative-neutral benchmark to allow the entity to assess the current state of privacy against the desired state.</p>
Implementing	<p>At this point, an action plan is mobilized and/or a diagnostic recommendation is put into effect. Implementing involves the execution of all planned and other tasks necessary to make the action plan operational. It includes the definition</p>	<p>Generally Accepted Privacy Principles can assist the entity in meeting its implementation goals. At the completion of the implementation phase, the entity should have developed the following deliverables:</p>

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	<p>of who will perform what tasks, assigning responsibilities, and establishing schedules/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.</p>	<ul style="list-style-type: none"> • Converted systems, procedures, and processes to address the privacy requirements • Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs
<p>Sustaining/Managing</p>	<p>Sustaining/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.</p>	<p>The entity can use Generally Accepted Privacy Principles, for example, 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.</p>
<p>Internal privacy audit</p>	<p>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.</p>	<p>Internal auditors can evaluate an entity's privacy program using Generally Accepted Privacy Principles as a benchmark and provide useful information and reporting to management.</p>
<p>External privacy audit</p>	<p>External auditors, notably CAs and CPAs, can perform assurance services. Generally, an external audit of financial and nonfinancial information builds trust and confidence for individuals, management, customers, business partners, and other users.</p>	<p>An external auditor can evaluate an entity's privacy program in accordance with Generally Accepted Privacy Principles and provide reports useful to individuals, management, customers, business partners, and other users.</p>

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 illustrations and explanations, which are designed to enhance the understanding of the criteria. 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 pertain to a certain industry or country.

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

Generally Accepted Privacy Principles and Criteria

Management

Ref.	Management Criteria	Illustrations and Explanations of Criteria	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: <ul style="list-style-type: none"> • Notice (See 2.1.0) • Choice and Consent (See 3.1.0) • Collection (See 4.1.0) • Use and Retention (See 5.1.0) • Access (See 6.1.0) • Onward Transfer and Disclosure (See 7.1.0) • Security (See 8.1.0) • Quality (See 9.1.0) • 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 policies are communicated to such personnel shortly after the changes	The entity: <ul style="list-style-type: none"> • Periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies and changes to its privacy policies. • Requires internal personnel to confirm (initially and periodically) their understanding of an agreement to comply with the 	Privacy policies encompass security policies relevant to the protection of personal information.

Ref.	Management Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	are approved.	entity's privacy policies. <ul style="list-style-type: none"> • Educates and trains internal personnel (initially and periodically) who have access to personal information or are charged with the security of personal information about privacy and security concepts, and issues; and promotes ongoing awareness. 	
1.1.2	<p>Responsibility and Accountability for Policies</p> <p>Responsibility and accountability are assigned to a person or group for 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.</p>	<p>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).</p> <p>The responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include:</p> <ul style="list-style-type: none"> • Establishing with management standards 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 	The individual identified as being accountable for privacy should be from within the entity.

Ref.	Management Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>practices</p> <p>The board periodically includes privacy in its regular review of corporate governance.</p> <p>The entity requires and documents users, management, and third-party confirmations (initially and annually) of their understanding and agreement to comply with the entity's privacy policies and procedures.</p>	
1.2	Procedures and Controls		
1.2.1	<p>Review and Approval Privacy policies and procedures and changes thereto are reviewed and approved by management.</p>	<p>Privacy policies and procedures are:</p> <ul style="list-style-type: none"> • Reviewed and approved by senior management or a management committee. • Reviewed at least annually and updated as needed. 	
1.2.2	<p>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 there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.</p>	<p>Corporate counsel or the legal department:</p> <ul style="list-style-type: none"> • Determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates. • Reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations. 	

Ref.	Management Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.2.3	<p>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.</p>	<p>Management and the corporate counsel or the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.</p>	
1.2.4	<p>Infrastructure and Systems Management Internal personnel or advisers review the design, acquisition, development, implementation, configuration, and management of:</p> <ul style="list-style-type: none"> • Infrastructure, • Systems, • Applications, • Web sites, and • Procedures, <p>and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.</p>	<p>Procedures are in place to:</p> <ul style="list-style-type: none"> • Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, disclose and destroy personal information. • Ensure that the entity's business continuity management processes are consistent with its privacy policies and procedures. • Classify the sensitivity of classes of data, and determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information. • Assess planned changes to systems and procedures for their potential effect on privacy. • Test changes to system components to minimize the risk of an adverse effect on the systems that process personal information. All test data are anonymized. • Require the documentation and approval by the privacy officer, 	

Ref.	Management Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>business unit manager and IT management before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis.</p> <p>The information technology (IT) department maintains a listing of all software and the respective level, version, and patches that have been applied.</p> <p>Procedures exist to provide that only authorized, tested, and documented changes are made to the system.</p>	
1.2.5	<p>Supporting Resources Resources are provided by the entity to implement and support its privacy policies.</p>	<p>Management reviews annually the assignment of personnel, budgets, and allocation of other resources to its privacy program.</p>	
1.2.6	<p>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.</p>	<p>The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as:</p> <ul style="list-style-type: none"> • Formal job descriptions (including responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions) • Hiring procedures (including the comprehensive screening of 	

Ref.	Management Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		credentials, background checks, and reference checking) <ul style="list-style-type: none"> • Training programs related to privacy and security matters • Performance appraisals (performed by supervisors, including assessments of professional development activities) 	
1.2.7	<p>Changes in Business and Regulatory Environments For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed:</p> <ul style="list-style-type: none"> • Business operations and processes • People • Technology • Legal • Contracts, including service-level agreements <p>Privacy policies and procedures are updated for such changes.</p>	<p>The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in:</p> <ul style="list-style-type: none"> • Business operations and processes • People assigned responsibility for privacy and security matters • Technology (prior to implementation) • Legal and regulatory environments • 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 corporate counsel before they are executed). 	

Notice

Ref.	Notice Criteria	Illustrations and Explanations of Criteria	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	<p>Communication to Individuals Notice is provided to individuals regarding the following privacy policies:</p> <ul style="list-style-type: none"> • Purpose for collecting personal information • Choice and Consent (See 3.1.1) • Collection (See 4.1.1) • Use and Retention (See 5.1.1) • Access (See 6.1.1) • Onward Transfer and Disclosure (See 7.1.1) • Security (See 8.1.1) • Quality (See 9.1.1) • Monitoring and Enforcement (See 10.1.1) <p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>	<p>The entity's privacy notice:</p> <ul style="list-style-type: none"> • Describes the purposes for which personal information is collected. • Indicates that the purpose for collecting sensitive personal information is part of a legal requirement. • May be provided in various ways (for example, in a face-to-face interview, a telephone interview, an application form or questionnaire, or electronically). Written notice is the preferred method. 	<p>Notice also may describe situations in which personal information will be disclosed, such as:</p> <ul style="list-style-type: none"> • Certain processing for purposes of public security or defense • Certain processing for purposes of public health or safety • When allowed or required by law <p>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.</p> <p>Consideration should be given to providing a summary level notice with links to more detailed sections of the policy.</p> <p>The use of "short notice" privacy statements is becoming more common. A short notice privacy statement is a separate page that</p>

Ref.	Notice Criteria	Illustrations and Explanations of Criteria	Additional Considerations
			succinctly highlights the scope, collection, use, choice, contact details, and other information relative to the information being collected in the particular business activity to which it is attached.
2.2	Procedures and Controls		
2.2.1	<p>Provision of Notice Notice is provided to the individual about the entity’s privacy policies and procedures:</p> <ul style="list-style-type: none"> ▪ At or before the time personal information is collected, or as soon as practical thereafter. ▪ At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter ▪ Before personal information is used for new purposes not previously identified. 	<p>Privacy notice is:</p> <ul style="list-style-type: none"> • 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. <p>In addition, the entity:</p> <ul style="list-style-type: none"> • 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 the mail, or by sending an e-mail. • Documents that changes to 	<p>See 3.2.2, “Consent for New Purposes and Uses.”</p> <p>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).</p>

Ref.	Notice Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>privacy policies and procedures were communicated to individuals.</p>	
2.2.2	<p>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.</p>	<p>The privacy notice describes the particular entities, business segments, locations, and types of information covered, for example:</p> <ul style="list-style-type: none"> • Operating jurisdictions (legal and 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) <p>The entity informs individuals when they might assume that 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).</p>	
2.2.3	<p>Clear and Conspicuous The entity's privacy notice is conspicuous and uses clear language.</p>	<p>The privacy notice is:</p> <ul style="list-style-type: none"> • In plain and simple language. • Appropriately labeled, easy to see, and not in fine print. • Linked to or displayed on the Web site at points of data collection. 	<p>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.</p>

Ref.	Notice Criteria	Illustrations and Explanations of Criteria	Additional Considerations
			<p>Some regulations, such as GLBA, may contain specific information that a disclosure must contain.</p> <p>Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure.</p>

Choice and Consent

Ref.	Choice and Consent Criteria	Illustrations and Explanations of Criteria	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: <ul style="list-style-type: none"> ▪ About the choices available to them with respect to the collection, use, and disclosure of personal information. ▪ That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise. 	The entity's privacy notice describes, in a clear and concise manner: <ul style="list-style-type: none"> • 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 that: <ul style="list-style-type: none"> • Personal information not essential to the purposes identified in the privacy notice need not be provided. • Preferences may be changed and consent may be withdrawn at a later time, subject to legal or 	Some laws and regulations (such as Principle 11, Limits on the 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: <ul style="list-style-type: none"> • The recordkeeper 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	Illustrations and Explanations of Criteria	Additional Considerations
		<p>contractual restrictions and reasonable notice.</p> <p>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).</p>	
3.1.2	<p>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.</p>	<p>The entity informs individuals at the time of collection:</p> <ul style="list-style-type: none"> • 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	<p>Implicit or Explicit Consent Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or as soon as practical thereafter. The</p>	<p>The entity:</p> <ul style="list-style-type: none"> • Obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is 	

Ref.	Choice and Consent Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>individual's preferences expressed in his or her consent are confirmed and implemented.</p>	<p>collected, or as soon as practical thereafter).</p> <ul style="list-style-type: none"> • 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	<p>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.</p>	<p>When personal information is to be used for a purpose not previously specified, the entity:</p> <ul style="list-style-type: none"> • 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 or, if consent was withdrawn, not so used. 	<p>If policies are changed but do not constitute new purposes or uses, the organization may wish to consult with legal counsel.</p>

Ref.	Choice and Consent Criteria	Illustrations and Explanations of Criteria	Additional Considerations
3.2.3	<p>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.</p>	<p>The entity collects sensitive information only if the individual provides explicit consent. <i>Explicit consent</i> 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.</p>	<p>The 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.</p> <p>Most jurisdictions referenced to in Attachment B, "Comparison of International Privacy Concepts," prohibit the collection of sensitive data, unless specifically allowed. For example, in the European Union (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.</p> <p>Some jurisdictions consider government-issued personal identifiers for example, Social Security numbers or Social Insurance numbers, to be sensitive information.</p>
3.2.4	<p>Consent for Online Data Transfers to/From an Individual's Computer Consent is obtained before personal information is transferred to/from an individual's computer.</p>	<p>The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer.</p> <p>If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that cookies are not stored on the customer's computer.</p>	<p>Consideration should be given to software that is designed to mine or extract information from a computer and therefore may be used to extract personal information, e.g., spyware.</p>

Ref.	Choice and Consent Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		Organizations will not download software that will transfer personal information without obtaining permission.	

Collection

Ref.	Collection Criteria	Illustrations and Explanations of Criteria	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 and the methods used to collect personal information.	
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.	Examples of the types of personal information collected are: <ul style="list-style-type: none"> • Financial (for example, financial account information) • Health (for example, information about physical or mental status or history) • Demographic (for example, age, income range, social geo-codes). Examples of methods of collecting and third-party sources of personal information are: <ul style="list-style-type: none"> • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons. The entity's privacy notice discloses that it uses cookies and Web beacons and how they are used. The notice also describes the consequences if the cookie is refused.	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

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

Ref.	Collection Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	relating to the collection of personal information.		<ul style="list-style-type: none"> To use a third party to collect information in order to avoid providing notice to individuals. <p>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).</p> <p>A review of complaints may help to identify whether there are unfair or unlawful practices.</p>
4.2.3	<p>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.</p>	<p>The entity:</p> <ul style="list-style-type: none"> Performs due diligence before establishing a relationship with a third-party data provider. Reviews the privacy policies and collection methods of third parties before accepting personal information from third-party data sources. 	<p>Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources.</p> <p>If information collected from third parties is to be combined with information collected from the individual, consideration should be given to providing notice to such individuals.</p>

Use and Retention

Ref.	Use and Retention Criteria	Illustrations and Explanations of Criteria	Additional Considerations
5.0	<p>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.</p>		
5.1	<p>Policies and Communications</p>		
5.1.0	<p>Privacy Policies The entity's privacy policies address the use and retention of personal information.</p>		
5.1.1	<p>Communication to Individuals Individuals are informed that personal information is:</p> <ul style="list-style-type: none"> ▪ 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. ▪ Retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation. 	<p>The entity's privacy notice describes the uses of personal information, for example:</p> <ul style="list-style-type: none"> • 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 <p>The entity's privacy notice explains that personal information will be</p>	

Ref.	Use and Retention Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.	
5.2	Procedures and Controls		
5.2.1	<p>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.</p>	<p>Systems and procedures are in place to ensure that personal information is used in:</p> <ul style="list-style-type: none"> • Conformity with the purposes identified in the entity’s privacy notice • Agreement with the consent received from the individual • Compliance with applicable laws and regulations. 	<p>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).</p>
5.2.2	<p>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. Personal information no longer retained is disposed and destroyed of in a manner that prevents loss, misuse, or unauthorized access.</p>	<p>The entity:</p> <ul style="list-style-type: none"> • Documents its retention policies and disposal procedures. • Erases or destroy records in accordance with the retention policies, regardless of the method of storage (for example, electronic or paper-based). • Retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies. • Ensures that personal information is not kept beyond the standard retention time unless there is a justified business reason for doing so. • Locates and removes specified personal information about an individual as required, for example, removing credit card 	<p>Some laws specify the retention period for personal information; for example, HIPAA has a six-year retention period from the date of creation or last in effect for personal information.</p> <p>There may be other statutory record retention requirements; for example, certain data may need to be retained for tax purposes or in accordance with employment laws.</p>

Ref.	Use and Retention Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>numbers after the transaction is complete.</p> <ul style="list-style-type: none"> 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. <p>Contractual requirements should be considered when establishing retention practices.</p>	

Access

Ref.	Access Criteria	Illustrations and Explanations of Criteria	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: <ul style="list-style-type: none"> • 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). 	
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: <ul style="list-style-type: none"> • 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 information, upon request, in printed or electronic form that is convenient to both the individual 	Some laws and regulations specify: <ul style="list-style-type: none"> • 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	Illustrations and Explanations of Criteria	Additional Considerations
		<p>and the entity.</p> <ul style="list-style-type: none"> Record requests for access, actions taken, including denial of access, and unresolved complaints and disputes. 	
6.2.2	<p>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.</p>	<p>Employees are adequately trained to authenticate the identity of individuals before granting:</p> <ul style="list-style-type: none"> Access to their personal information Requests to change sensitive or other personal information (for example, to update information such as address or bank details). <p>The entity:</p> <ul style="list-style-type: none"> 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 user identification (ID) and password (or equivalent) be used to access user account information online. 	<p>The extent of authentication considers the type and sensitivity of personal information that is made available. Different techniques may be considered for the different channels:</p> <ul style="list-style-type: none"> Web Interactive voice response system Call center In person
6.2.3	<p>Understandable Personal Information, Time Frame, and Cost Personal information is provided to the individual in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.</p>	<p>The entity:</p> <ul style="list-style-type: none"> Provides personal information to the individual in a format that is understandable (for example, not in code, not in a series of numbers, not in overly technical language or other jargon) and in 	<p>Entities may provide individuals with access to their personal information at no cost or at a minimal cost because of the potential business and customer-relationship benefits as well as the opportunity to enhance the quality of the information.</p>

Ref.	Access Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>a form convenient to both the individual and the entity.</p> <ul style="list-style-type: none"> • 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 time frame 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. 	
6.2.4	<p>Denial of Access Individuals are informed, in writing, of the reason a request for access to</p>	<p>The entity:</p> <ul style="list-style-type: none"> • Outlines the reasons why access to personal information may be 	<p>Some laws and regulations (for example, Principle 5, "Information Relating to Records Kept by Record-</p>

Ref.	Access Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>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.</p>	<p>denied.</p> <ul style="list-style-type: none"> 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 as to why access to personal information is denied. Provides a formal escalation and review process if access to personal information is denied. (See 6.2.7, "Escalation of Complaints and Disputes"). Conveys the entity's legal rights and the individual's right to challenge, if applicable. 	<p>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.</p>
6.2.5	<p>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.</p>	<p>The entity:</p> <ul style="list-style-type: none"> 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). Records the date, time, and identification of the person making the change if the entity's 	<p>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.</p>

Ref.	Access Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>employee is making a change on behalf of an individual.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>	<p>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.</p> <p>The entity:</p> <ul style="list-style-type: none"> • 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 its refusal by the entity. • If appropriate, notifies third parties who have previously been 	<p>Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of disagreements from individuals.</p> <p>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.</p>

Ref.	Access Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		provided with personal information that there is a disagreement.	
6.2.7	<p>Escalation of Complaints and Disputes Complaints and other disputes are escalated until they are resolved.</p>	<p>The entity has established a formal escalation process to address complaints and disputes that are not resolved.</p> <p>The entity:</p> <ul style="list-style-type: none"> • Trains employees responsible for handling individuals' complaints and disputes about the escalation process. • Documents unresolved complaints and disputes. • Escalates complaints and disputes for review by management. • Resolves complaints and disputes on a timely basis. • Engages an external, third-party dispute resolution service (for example, an arbitrator), when appropriate, to assist in the resolution of complaints and disputes. 	<p>See 10.1.1, "Communications to Individuals", 10.2.1, "Complaint Process", and 10.2.2, "Dispute Resolution and Recourse."</p> <p>Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.</p>

Disclosure to Third Parties

Ref.	Disclosure to Third Parties Criteria	Illustrations and Explanations of Criteria	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: <ul style="list-style-type: none"> • 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 (1) identified in the notice and (2) 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: <ul style="list-style-type: none"> • 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 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 to and obtains a written agreement from the third party that its data protection practices are substantially equivalent to the entity's.	

Ref.	Disclosure to Third Parties Criteria	Illustrations and Explanations of Criteria	Additional Considerations
<p>7.2</p> <p>7.2.1</p>	<p>Procedures and Controls</p> <p>Disclosure of Personal Information</p> <p>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 allows or requires otherwise.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • 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. 	<p>Personal information may be disclosed through various legal processes to law enforcement or regulatory agencies.</p> <p>Some laws and regulations have specific provisions for the disclosure of personal information. Some permit disclosure of personal information without consent while others require verifiable consent.</p>
<p>7.2.2</p>	<p>Protection of Personal Information</p> <p>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.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • Provide a level of protection of personal information equivalent to that of the entity when information is provided to a third party (that is, by contract or agreement). • Affirm that the level of protection of personal information by third parties is equivalent to that of the entity, for example, by obtaining assurance (for example, an auditor's report), contractual obligation, or other representation (for example, written annual confirmation). • Limit the third party's use of personal information to purposes 	<p>The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party.</p> <p>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.</p> <p>Some jurisdictions, including some countries in Europe, require entities that transfer personal information to register with their regulatory body prior to transfer.</p>

Ref.	Disclosure to Third Parties Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>necessary to fulfill the contract.</p> <ul style="list-style-type: none"> • Communicate the individual's preferences to the third party. • Refer any requests for access or complaints about the personal information transferred by the entity to a designated privacy executive, such as a corporate privacy officer. • Specify how and when third parties are to dispose of or return any personal information provided by the entity. 	<p>PIPEDA requires a comparable level of protection while the personal information is being processed by a third party.</p> <p>Article 25 of the EU's Directive requires that such transfers take place only where the third party ensures an adequate level of protection.</p>
7.2.3	<p>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.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • 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 specified in the privacy notice. 	<p>Other types of onward transfers include transfers to third parties who are:</p> <ul style="list-style-type: none"> • 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.
7.2.4	<p>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.</p>	<p>The entity:</p> <ul style="list-style-type: none"> • 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 	

Ref.	Disclosure to Third Parties Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>arrangements.</p> <ul style="list-style-type: none"> • Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (For example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers). • 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	Illustrations and Explanations of Criteria	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 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: <ul style="list-style-type: none"> • 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. • Special 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	Illustrations and Explanations of Criteria	Additional Considerations
8.2.1	<p>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.</p>	<p>The entity's security program addresses the following matters related to protection of personal information:</p> <ul style="list-style-type: none"> • Periodic risk assessments • 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 • Implementing system software upgrades and patches • Testing, evaluating, and authorizing system principles 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 	<p>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.</p> <p>Some regulations (for example, HIPAA) provide a greater level of detail and guidance on specific security measures to be considered and implemented.</p> <p>Some security rules (for example, GLBA-related rules for safeguarding information) require:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▪ Exercising appropriate due diligence in the selection of service providers. ▪ Requiring service providers by contract to implement and maintain appropriate safeguards for the personal information at issue. <p>Some security laws (for example, California SB1386) require entities to notify individuals if the protection of their personal information is</p>

Ref.	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>into systems and to proactively test security procedures (for example, penetration testing)</p> <ul style="list-style-type: none"> • 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 • 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 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 <p>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 (e.g., computers, media and paper-based information in storage, sold, or otherwise disposed of).</p>	<p>compromised.</p> <p>Payment card issuers have established security and privacy requirements.</p>

Ref.	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
8.2.2	<p>Logical Access Controls Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> • Authorizing and registering internal personnel and individuals • Identifying and authenticating internal personnel and individuals • Making changes and updating access profiles • Granting system access privileges and permissions • Preventing individuals from accessing other than their own personal or sensitive information • Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities • Distributing output only to authorized internal personnel • Restricting logical access to offline storage, backup data, systems, and media • Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) • Preventing the introduction of viruses, malicious code, and unauthorized software 	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • 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. • Require the user to provide a valid ID and password to be authenticated by the system before access is granted to systems handling personal information. • Require enhanced security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls. • Implement intrusion detection and monitoring systems. 	<p>User authorization processes consider:</p> <ul style="list-style-type: none"> • 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.
8.2.3	<p>Physical Access Controls Physical access is restricted to</p>	<p>Systems and procedures are in place to:</p>	<p>Physical safeguards may include the use of locked file cabinets, card</p>

Ref.	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>personal information in any form (including the principles of the entity's system(s) that contain or protect personal information).</p>	<ul style="list-style-type: none"> • 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 attempts to gain unauthorized access. • Communicate investigation results to 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). 	<p>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.</p>
<p>8.2.4</p>	<p>Environmental Safeguards Personal information, in all forms, is protected against unlawful destruction, accidental loss, natural disasters, and environmental hazards.</p>	<p>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. Water detectors are installed within the raised floor areas.</p> <p>The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and</p>	

Ref.	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		emergency power supplies. This equipment is tested semiannually.	
8.2.5	<p>Transmitted Personal Information Personal information is protected when transmitted by mail and over the Internet and public networks by deploying industry standard encryption technology for transferring and receiving personal information.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • Address the confidentiality of information and communication, and the appropriate protection of personal information transmitted over the Internet or other public networks. • Define minimum levels of encryption and controls. • Employ industry standard encryption technology, for example, 128 bit secure socket layer (SSL), for transferring and receiving personal information. • Approve external network connections. • Protect personal information sent by mail, courier, or other physical means. 	<p>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).</p> <p>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.</p> <p>As technology, market, and regulatory conditions evolve, new measures may become necessary to meet acceptable levels of protection (for example, 128-bit SSL encryption, including user IDs and passwords).</p>
8.2.6	<p>Testing Security Safeguards Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • 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 	<p>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.</p> <p>Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to:</p> <ul style="list-style-type: none"> • Conduct regular tests of key

Ref.	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>other physical security devices at least annually.</p> <ul style="list-style-type: none"> • Document and test disaster recovery and contingency plans at least annually to ensure their viability. • Periodically undertake threat and vulnerability testing, including security penetration reviews 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. 	<p>controls, systems, and procedures by independent third parties or by staff independent of those that develop or maintain security (or at least have these independent parties review results of testing).</p> <ul style="list-style-type: none"> • Assess and possibly adjust its information security at least annually.

Quality

Ref.	Quality Criteria	Illustrations and Explanations of Criteria	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.	<p>The entity's privacy notice explains that the extent to which personal information is kept accurate and complete depends on the use of the information.</p> <p>Accurate directions are presented by the entity to inform individuals as to what information is needed to complete a transaction and what information is optional.</p>	
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.	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • 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 	

Ref.	Quality Criteria	Illustrations and Explanations of Criteria	Additional Consideration
		<p>update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information).</p> <ul style="list-style-type: none"> 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 there are clear limits to 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. <p>The entity undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary.</p>	
9.2.2	<p>Relevance of Personal Information Personal information is relevant to the purposes for which it is to be used.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> Ensure personal information is sufficiently relevant for the purposes for which it is to be used and to minimize the possibility that inappropriate 	

Ref.	Quality Criteria	Illustrations and Explanations of Criteria	Additional Consideration
		<p>information is used to make business decisions about the individual.</p> <ul style="list-style-type: none"> 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	Illustrations and Explanations of Criteria	Additional Considerations
10.0	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related 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 complaints.	The entity's privacy notice: <ul style="list-style-type: none"> • 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	Complaint Process A process is in place to address complaints.	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 set out: <ul style="list-style-type: none"> • Procedures to be followed in communicating and resolving complaints about the entity 	

Ref.	Monitoring and Enforcement Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> Action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved Remedies available in case of a breach of personal information and how to communicate this information to an individual Recourse available and formal escalation process 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	<p>Dispute Resolution and Recourse Every complaint is addressed and the resolution is documented and communicated to the individual.</p>	<p>The entity has a formally documented process in place to:</p> <ul style="list-style-type: none"> Record and respond to all complaints in a timely manner. Periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner. Identify trends and the potential need to change the entity's privacy policies and procedures. Address complaints that cannot be resolved. Use specified independent third-party dispute resolution services or other process mandated by regulatory bodies in the event the individual is not satisfied with the entity's proposed resolution, together with a commitment 	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements.

Ref.	Monitoring and Enforcement Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>from such third parties to handle such recourses.</p> <p>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.</p>	
10.2.3	<p>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, the entity's privacy policies and procedures are enforced.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • Annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts. • Document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-off, are maintained. • 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 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	<p>Instances of Noncompliance Instances of noncompliance with</p>	<p>Systems and procedures are in place to:</p>	

Ref.	Monitoring and Enforcement Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>privacy policies and procedures are documented and reported and, if needed, corrective measures are taken on a timely basis.</p>	<ul style="list-style-type: none"> • 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. • Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers). • Identify trends that may require revisions to privacy policies and procedures. 	

Appendix A - Glossary

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

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 either orally 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 (see [opt in](#) and [opt out](#), below).

Cookies. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. This 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.

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. There is implied consent 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.

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

Privacy. The rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention 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 Generally Accepted Privacy Principle and Criteria.

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

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, 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.

Appendix B - Comparison of International Privacy Concepts

The table below presents a comparison of privacy concepts set out in some domestic and international privacy regulations, laws, and guidelines in relation to Generally Accepted Privacy Principles. This is for illustrative purposes only and not meant to be comprehensive. Column 1 lists the 10 principles of Generally Accepted Privacy Principles. Columns 2 through 9 lists the significant principles discussed in specific laws and regulations. The “Key to Column and Source,” that follows the table identifies the source of each law and regulation compared:

<i>(1)</i> Generally Accepted Privacy Principles	<i>(2)</i> Australia Privacy Act	<i>(3)</i> Canada PIPEDA	<i>(4)</i> E.U. Directive	<i>(5)</i> OECD Guidelines	<i>(6)</i> U.S. FTC	<i>(7)</i> U.S. Safe Harbor	<i>(8)</i> U.S. HIPAA	<i>(9)</i> U.S. GLBA
Management		Accountability	Notification	Accountability			Administrative requirements	
Notice	Openness	Identifying Purposes, Openness	Information to Be Given to the Data Subject	Purpose Specification, Openness	Notice	Notice	Notice	Privacy and Opt Out Notices, Exceptions
Choice and Consent	Use and Disclosure	Consent	Criteria for Making Data Processing Legitimate, Data Subject’s Right to Object	Collection Limitation	Choice	Choice	Consent, Uses and Disclosures	Privacy and Opt Out Notices
Collection	Collection, Sensitive Information, Anonymity	Limiting Collection	Principles Relating to Data Quality, Exemptions and Restrictions	Collection (including consent) Limitation		Data Integrity		
Use and Retention	Identifiers, Use and Disclosure	Limiting Use, Disclosure, and Retention	Making Data Processing Legitimate, Special Categories of	Use Limitation (including disclosure limitation)		(Implied but not specified in the principles)	Uses and Disclosures	Limits on Disclosures

(1) Generally Accepted Privacy Principles	(2) Australia Privacy Act	(3) Canada PIPEDA	(4) E.U. Directive	(5) OECD Guidelines	(6) U.S. FTC	(7) U.S. Safe Harbor	(8) U.S. HIPAA	(9) U.S. GLBA
			Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object					
Access	Access and Correction	Individual Access	The Data Subject's Right of Access to Data	Individual Participation		Access	Access	
Disclosure to Third Parties	Use and Disclosure, Transborder Data Flows	Limiting Use, Disclosure, and Retention	Transfer of Personal Data to Third Countries	Use Limitation (including disclosure limitation)		Onward Transfer	Uses and Disclosures, Accounting of Disclosures	Limits on Disclosures
Security	Data Security	Safeguards	Confidentiality and Security of Processing	Security Safeguards	Security	Security	Security Rule	Security Guidelines mandated by section 501(b) of GLBA
Quality	Data Quality	Accuracy	Principles Relating to Data Quality	Data Quality	Integrity	Data Integrity	Amendment	
Monitoring and Enforcement	Enforcement by the Office of the Privacy Commissioner	Challenging Compliance	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation (including challenging compliance)	Enforcement	Enforcement	Compliance and Enforcement by the Department of Health and Human Services	Enforcement by financial services industry regulators, the FTC, and SEC

Key to Column and Source

(1) AICPA/CICA Generally Accepted Privacy Principles, May 2006.

(2) Australia Privacy Act 1988, *Privacy Act 1988*, as amended, effective December 21, 2001.

(3) Canada *Personal Information Protection and Electronic Documents Act* (PIPEDA), also referred to as. Bill C-6, Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, 1999-2000, assented to April 13, 2000, effective January 1, 2001.

(4) EU Directive, European Union (EU), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, October 24, 1995, effective October 25, 1998, as implemented in EU country-specific laws and regulations.

(5) OECD Guidelines, Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.

(6) U.S. FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, United States (U.S.) Federal Trade Commission (FTC), May 2000.

(7) U.S. Safe Harbor, an agreement between the U.S. Department of Commerce and the European Commission's Internal Market Directorate, approved by the European Commission July 27, 2000, open for use November 1, 2000.

(8) U.S. United States Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy Rule (compliance deadline April 16, 2003), Security Rule (compliance deadline April 21, 2005).

(9) U.S. Financial Services Modernization Act, also referred to as the Gramm-Leach-Bliley Act (GLBA), Title V – Privacy, Subtitle A, enacted November 12, 1999, effective November 13, 2000, Compliance by July 1, 2001. The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (collectively, the Agencies) published final Guidelines establishing standards for safeguarding customer information that implement sections 501 and 505(b) of GLBA.