

Trust Services Privacy Components and Criteria

[Management](#)

[Notice](#)

[Choice and Consent](#)

[Collection](#)

[Use and Retention](#)

[Access](#)

[Disclosure to Third Parties](#)

[Security](#)

[Quality](#)

[Monitoring and Enforcement](#)

Management

Ref.	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	<p>Privacy Policies</p> <p>The entity defines and documents its privacy policies with respect to:</p> <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	<p>Privacy policies are documented (in writing) and made readily available to internal personnel and third parties who need them.</p>	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>8.1.0)</p> <ul style="list-style-type: none"> • Quality (See 9.1.0) • Monitoring and Enforcement (See 10.1.0) 		
1.1.1	<p>Communication to Internal Personnel</p> <p>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 are approved.</p>	<p>The entity:</p> <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 entity's privacy policies. • 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 awareness, concepts, and issues. 	<p>Privacy policies encompass security policies relevant to the protection of personal information.</p>
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</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 authority and</p>	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>names of such person or group and their responsibilities are communicated to internal personnel.</p>	<p>accountability of the designated person or group are clearly documented. Responsibilities include:</p> <ul style="list-style-type: none"> • Establishing 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 practices. <p>The Board periodically includes privacy in its regular review of corporate governance.</p> <p>The entity requires users, management, and third parties to 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>	
1.2	Procedures and		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	Controls		
1.2.1	<p>Review and Approval</p> <p>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</p> <p>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. 	
1.2.3	<p>Consistency of Commitments With Privacy Policies and Procedures</p> <p>Entity personnel or advisors 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>	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.2.4	<p>Infrastructure and Systems Management</p> <p>Entity personnel or advisors review the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures 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, and disclose personal information. • Ensure that the entity's backup and disaster-recovery planning 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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>documentation and approval by the privacy officer and business unit manager 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</p> <p>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 Personnel</p> <p>The entity establishes qualifications for personnel responsible for protecting the privacy and security</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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.</p>	<p>descriptions (including responsibilities, educational and professional requirements and organizational reporting for key privacy management positions)</p> <ul style="list-style-type: none"> • Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) • 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</p> <p>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>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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	Privacy policies and procedures are updated for such changes.	clauses in contracts are reviewed and approved by the privacy officer or corporate counsel before they are executed.)	

[Back to top](#)

Notice

Ref.	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	Communication to Individuals Notice is provided to individuals regarding the following privacy policies: <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) 	The entity's privacy notice: <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. 	Notice also may describe situations in which personal information will be disclosed, such as: <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 The purpose described in the notice should be stated in such a

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>		<p>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>
2.2	Procedures and Controls		
2.2.1	<p>Provision of Notice</p> <p>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 (See 3.2.2, “Consent for New Purposes and Uses.”) 	<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>	<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.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<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 privacy policies and procedures were communicated to individuals. 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
2.2.2	<p>Entities and Activities Covered</p> <p>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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>example, mail order or online)</p> <p>The entity informs individuals when they leave the Web site and are no longer covered by the entity's privacy policies and procedures.</p>	
2.2.3	<p>Clear and Conspicuous</p> <p>Clear and conspicuous language is used in the entity's privacy notice.</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 should be encouraged to avoid consumer confusion and clarify their understanding of any differences.</p> <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>

[Back to top](#)

Choice and Consent

Ref.	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		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>The entity's privacy policies address the choices available to individuals and the consent to be obtained.</p>		
3.1.1	<p>Communication to Individuals</p> <p>Individuals are informed:</p> <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. 	<p>The entity's privacy notice describes, in a clear and concise manner:</p> <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 consequences of failing to provide personal information <p>Individuals are advised that:</p> <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 contractual restrictions and reasonable notice. <p>The type of consent required depends on the nature of the personal information and the method of</p>	<p>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:</p> <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.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the entity).	
3.1.2	<p>Consequences of Denying or Withdrawing Consent</p> <p>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</p> <p>Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or as soon as practical thereafter.</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 collected, or as soon as practical thereafter). 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	The individual's preferences expressed in his or her consent are confirmed and implemented.	<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. • Addresses conflicts in the records about an individual's 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</p> <p>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. 	If policies are changed but do not constitute new purposes or uses, the organization may wish to consult with legal counsel.
3.2.3	<p>Explicit Consent for Sensitive Information</p> <p>Explicit consent is obtained directly from</p>	The entity collects sensitive information only if the individual provides explicit consent. Explicit	The Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1,

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.</p>	<p>consent requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.</p>	<p>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 D, "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 that "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained.</p>
3.2.4	<p>Consent for Online Data Transfers to/from an Individual's Computer</p> <p>Consent is obtained before personal information is transferred to/from an individual'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>The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer.</p> <p>Organizations will not</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.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		download software that will transfer personal information without obtaining permission.	

[Back to top](#)

Collection

Ref.	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-	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>party sources of personal information are:</p> <ul style="list-style-type: none"> • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons. <p>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.</p>	
4.2	Procedures and Controls		
4.2.1	<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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.	
4.2.2	<p>Collection by Fair and Lawful Means</p> <p>Methods of collecting personal information are reviewed by management, legal counsel, or both before they are implemented to confirm that personal information is obtained:</p> <ul style="list-style-type: none"> • Fairly, without intimidation or deception. • Lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information. 	<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. • 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>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
4.2.3	<p>Collection From Third Parties</p> <p>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>

[Back to top](#)

Use and Retention

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
5.0	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.		
5.1	Policies and Communications		
5.1.0	<p>Privacy Policies</p> <p>The entity's privacy policies address the use and retention of personal information.</p>		
5.1.1	<p>Communication to Individuals</p> <p>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 	<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, 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.</p> <ul style="list-style-type: none"> Retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation. 	<p>or other compensation schemes.</p> <ul style="list-style-type: none"> 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 retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.</p>	
5.2	Procedures and Controls		
5.2.1	<p>Use of Personal Information</p> <p>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 monitor the use of personal information to ensure:</p> <ul style="list-style-type: none"> Use in conformity with the purposes identified in the entity's privacy notice. Use in agreement with the consent received from the individual Compliance with 	<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>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		applicable laws and regulations	
5.2.2	<p>Retention of Personal Information</p> <p>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 numbers after the transaction is complete. • Regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or required by laws and regulations. <p>Contractual requirements should be considered when establishing retention practices.</p>	<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>

[Back to top](#)

Access

Ref.	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. 	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.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> • 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 and the entity. • 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</p> <p>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. 	<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

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> • Requires that a user identification (ID) and password (or equivalent) be used to access user account information online. 	
6.2.3	<p>Understandable Personal Information, Time Frame, and Cost</p> <p>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 a form convenient to both the individual and the entity. • Makes a reasonable effort to locate the personal information requested and, if personal information cannot be found, keeps sufficient records to demonstrate that a reasonable search was made. • Takes reasonable precautions to ensure that personal information released does not identify another person, directly or indirectly. • Provides access to personal information in a 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 	<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.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>personal information in archived or backup systems and media.</p> <ul style="list-style-type: none"> • 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, that 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</p> <p>Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.</p>	<p>The entity:</p> <ul style="list-style-type: none"> • Outlines the reasons why access to personal information may be denied. • Records all denials of access and unresolved complaints and disputes. • Provides the individual with partial access in situations in which access to some of his or her personal information is justifiably denied. • Provides the individual with a written explanation 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. 	<p>Some laws and regulations (for example, Principle 5, "Information Relating to Records Kept by Record-Keeper," point 2 of the Australian Privacy Act of 1988 and PIPEDA, Sections 8.(4), 8.(5), 8.(7), 9, 10 and 28) specify the situations in which access can be denied, the process to be followed (such as notifying the customer of the denial in writing within 30 days), and potential penalties or sanctions for lack of compliance.</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>“Escalation of Complaints and Disputes.”)</p> <ul style="list-style-type: none"> • Conveys the entity’s legal rights and the individual’s right to challenge, if applicable. 	
6.2.5	<p>Updating or Correcting Personal Information</p> <p>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 employee is making a change on behalf of an individual. • Notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so. 	<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>
6.2.6	<p>Statement of Disagreement</p> <p>Individuals are informed, in writing,</p>	<p>If an individual and an entity disagree about whether personal information is complete and accurate, the</p>	<p>Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>about the reason a request for correction of personal information was denied, and how they may appeal.</p>	<p>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 provided with personal information that there is a disagreement. 	<p>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>
6.2.7	<p>Escalation of Complaints and Disputes</p> <p>Complaints and other disputes are escalated</p>	<p>The entity has established a formal escalation process to address complaints and disputes that are not resolved.</p>	<p>Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	until they are resolved.	<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. 	

[Back to top](#)

Disclosure to Third Parties

Ref.	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	<p>Privacy Policies</p> <p>The entity's privacy policies address the disclosure of personal information to third parties.</p>		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
7.1.1	<p>Communication to Individuals</p> <p>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. Disclosure includes any limitation on the third party's privacy practices and controls. Lack of such disclosure indicates that the third party's privacy practices and controls meet or exceed those of the entity.</p>	<p>The entity's privacy notice:</p> <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. • Individuals are informed if third parties provide lower levels of protection. 	<p>The entity's privacy notice may disclose:</p> <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	<p>Communication to Third Parties</p> <p>Privacy policies are communicated to third parties to whom personal information is disclosed.</p>	<p>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 practices are substantially equivalent to the entity's.</p>	
7.2	<p>Procedures and Controls</p>		
7.2.1	<p>Disclosure of Personal Information</p>	<p>Systems and procedures are in place to:</p>	<p>Personal information may be disclosed through various legal</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<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>	<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>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>
7.2.2	<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 from loss, misuse, unauthorized access, disclosure, alteration, and destruction.</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). 	<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>The EU requires substantially equivalent privacy protection before transferring</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> • Limit the third party's use of personal information to purposes necessary to fulfill the contract. • 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 the privacy officer. • Specify how and when third parties are to dispose of or return any personal information provided by the entity. 	<p>personal information to a third party.</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> <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 U.S./EU's Safe Harbor 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</p> <p>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.

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
7.2.4	<p>Misuse of Personal Information by a Third Party</p> <p>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"> • Monitors complaints to identify indications of any misuse of personal information by third parties. • Responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements. • Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures. • 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.) 	

[Back to top](#)

Security

Ref.	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		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	Communications		
8.1.0	<p data-bbox="347 329 553 359">Privacy Policies</p> <p data-bbox="347 394 613 516">The entity's privacy policies address the security of personal information.</p>	<p data-bbox="686 329 1000 678">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.</p>	<p data-bbox="1034 329 1347 516">Personal information in any location under control of the entity or deemed to be under control of the entity must be protected.</p>
8.1.1	<p data-bbox="347 749 594 810">Communication to Individuals</p> <p data-bbox="347 846 639 999">Individuals are informed that precautions are taken to protect personal information.</p>	<p data-bbox="686 749 1000 999">The entity's privacy notice describes the general types of security measures used to protect the individual's personal information, for example:</p> <ul data-bbox="686 1041 1000 1776" 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. 	<p data-bbox="1034 749 1347 1062">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.</p> <p data-bbox="1034 1104 1347 1388">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.</p> <p data-bbox="1034 1430 1347 1612">Consideration should be given to limiting the disclosure of detailed security procedures so as not to compromise internal security.</p>
8.2	Procedures and Controls		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
8.2.1	<p>Information Security Program</p> <p>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"> a. Periodic risk assessments b. Identification and documentation of the security requirements of authorized users c. Allowing access, the nature of that access, and who authorizes such access. d. Preventing unauthorized access by using effective physical and logical access controls. e. The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access f. Assignment of responsibility and accountability for security. g. Assignment of responsibility and accountability for system changes and maintenance. h. Implementing system software upgrades and patches. i. Testing, evaluating, and authorizing system components before implementation. j. Addressing how complaints and 	<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

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>requests relating to security issues are resolved.</p> <ul style="list-style-type: none"> k. Handling errors and omissions, security breaches, and other incidents. l. Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing). m. Allocating training and other resources to support its security policies. n. Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies. o. Disaster recovery plans and related testing. p. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts. q. A requirement that users, management, and third parties confirm (initially and annually) their 	<p>implement and maintain appropriate safeguards for the personal information at issue.</p> <p>Some security laws (for example, California SB1386) require entities to notify individuals if the protection of their personal information is compromised.</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information.</p> <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>	
8.2.2	<p>Logical Access Controls</p> <p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ol style="list-style-type: none"> a. Authorizing and registering internal personnel and individuals b. Identifying and authenticating internal personnel and individuals c. Making changes and updating access profiles d. Granting system access privileges and permissions e. Preventing individuals from accessing other 	<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 	<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.

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>than their own personal or sensitive information</p> <p>f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities</p> <p>g. Distributing output only to authorized internal personnel</p> <p>h. Restricting logical access to offline storage, backup data, systems, and media</p> <p>i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</p> <p>j. Preventing the introduction of viruses, malicious code, and unauthorized software</p>	<p>security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, or secure ID cards, virtual private network (VPN), properly configured firewalls.</p> <ul style="list-style-type: none"> • Implement intrusion detection and monitoring systems. 	
8.2.3	<p>Physical Access Controls</p> <p>Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).</p>	<p>Systems and procedures are in place to:</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. 	<p>Physical safeguards may include the use of locked file cabinets, card access systems, physical keys, sign-in logs, and other techniques to control access to offices, data centers, and other locations in which personal information is processed or stored.</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> • Prevent the unauthorized or accidental destruction or loss of personal information. • Investigate breaches and attempts to gain unauthorized access. • Maintain physical control over the distribution of reports containing personal information. • Securely dispose of waste containing confidential information (for example, shredding). 	
8.2.4	<p>Environmental Safeguards</p> <p>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 emergency power supplies. This equipment is tested semiannually.</p>	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
8.2.5	<p>Transmitted Personal Information</p> <p>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</p> <p>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 	<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</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>security controls using either internal or external auditors.</p> <ul style="list-style-type: none"> • Test card access systems and other physical security devices at least annually. • 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>example, GLBA-related rules for safeguarding information) require an entity to:</p> <ul style="list-style-type: none"> • Conduct regular tests of key 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). • Assess and possibly adjust its information security at least annually.

[Back to top](#)

Quality

Ref.	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.	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.	
9.2	Procedures and Controls		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Consideration
9.2.1	<p data-bbox="296 342 613 435">Accuracy and Completeness of Personal Information</p> <p data-bbox="296 472 613 597">Personal information is accurate and complete for the purposes for which it is to be used.</p>	<p data-bbox="638 342 961 435">Systems and procedures are in place to:</p> <ul data-bbox="638 472 961 1369" style="list-style-type: none"> <li data-bbox="638 472 961 630">• Edit and validate personal information as it is collected, created, maintained, and updated. <li data-bbox="638 634 961 760">• Record the date when the personal information is obtained or updated. <li data-bbox="638 764 961 1117">• Specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information). <li data-bbox="638 1122 961 1369">• 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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Consideration
		<p>Third Parties”), or disclosed to a third party (see 7.2.2, “Protection of Personal Information”).</p> <ul style="list-style-type: none"> • 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	Relevance of Personal Information	Systems and procedures are in place to:	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Consideration
	Personal information is relevant to the purposes for which it is to be used.	<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 information is used to make business decisions about the individual. • 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.	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		

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.		
10.1.1	<p>Communication to Individuals</p> <p>Individuals are informed about how to contact the entity with complaints.</p>	<p>The entity's privacy notice:</p> <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	The corporate privacy officer or other	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	A process is in place to address complaints.	<p>designated individual is authorized to address privacy-related complaints, disputes, and other problems.</p> <p>Systems and procedures are in place that set out:</p> <ul style="list-style-type: none"> • Procedures to be followed in communicating and resolving complaints about the entity. • 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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>approve any recourse offered to individuals.</p> <ul style="list-style-type: none"> • 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</p> <p>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- 	<p>Some regulations (for example HIPAA and COPPA) have specific procedures and requirements.</p>

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>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 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</p> <p>Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • Annually review compliance with privacy policies and 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>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>procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts.</p> <ul style="list-style-type: none"> • 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 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		revised, as necessary).	
10.2.4	<p>Instances of Noncompliance</p> <p>Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective measures are taken on a timely basis.</p>	<p>Systems and procedures are in place to:</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. • Identify trends that may require revisions to privacy policies and procedures. 	

Ref.	Criteria	Illustrations and Explanations of Criteria	Additional Considerations

[Back to top](#)