Last Updated: August 2023

Safeguarding Personal Information

	PIPEDA	PIPA Alberta	PIPA British Columbia	Quebec Private Sector Privacy Act (as amended by Law 25)
Security safeguards	**Principle 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. **Principle 7 — Safeguards** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **4.7.1** The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.	**s. 34** An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.	**s. 34** An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.	**s. 3.1** Any person carrying on an enterprise is responsible for protecting the personal information held by the person. […] **s. 10** A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

	PIPEDA	PIPA Alberta	PIPA British Columbia	Quebec Private Sector Privacy Act (as amended by Law 25)
	Organizations shall protect personal information regardless of the format in which it is held. **4.7.2** The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4. **4.7.3** The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access			

	PIPEDA	PIPA Alberta	PIPA British Columbia	Quebec Private Sector Privacy Act (as amended by Law 25)
	on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption.			
Methods of protection	**s. 4.7.3** The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption.	**N/A**	**N/A**	**s. 20** In the carrying on of an enterprise, authorized employees or agents may have access to personal information without the consent of the person concerned only if the information is needed for the performance of their duties. **s. 25 of the *Act to establish a legal framework for information technology*, CQLR c C-1.1.** The person responsible for access to a technology-based document containing confidential information must take appropriate security measures to protect its confidentiality, such as controlling access to the

	PIPEDA	PIPA Alberta	PIPA British Columbia	Quebec Private Sector Privacy Act (as amended by Law 25)
				document by means of a restricted view technique, or any technique that prevents unauthorized persons from accessing such information or from otherwise accessing the document or the components providing access to the document. **s. 26 of the *Act to establish a legal framework for information technology*, CQLR c C-1.1.** Anyone who places a technology-based document in the custody of a service provider is required to inform the service provider beforehand as to the privacy protection required by the document according to the confidentiality of the information it contains, and as to the persons who are authorized to access the document.

	PIPEDA	PIPA Alberta	PIPA British Columbia	Quebec Private Sector Privacy Act (as amended by Law 25)
				During the period the document is in the custody of the service provider, the service provider is required to see to it that the agreed technological means are in place to ensure its security and maintain its integrity and, if applicable, protect its confidentiality and prevent accessing by unauthorized persons. Similarly, the service provider must ensure compliance with any other obligation provided for by law as regards the retention of the document.
Employee awareness	**s. 4.7.4** Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.	**N/A**	**N/A**	**N/A**

Care in disposal or destruction of personal information	**s. 4.7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).	**N/A**	**N/A**	**s. 3.2** Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must, in particular, provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise's activities and be approved by the person in charge of the protection of personal information.[…] **s. 23** Where the purposes for which personal information was collected or used are achieved,

				the person carrying on an enterprise must destroy the information, or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act. For the purposes of this Act, information concerning a natural person is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly. Information anonymized under this Act must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation.