646A.622 Requirement to develop safeguards for personal information; conduct deemed to comply with requirement. (1) A person that owns, maintains or otherwise possesses data that includes a consumer's personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information.

(2) A person complies with subsection (1) of this section if the person:

(a) Complies with a state or federal law that provides greater protection to personal information than the protections that this section provides.

(b) Complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as in effect on January 1, 2016, if the person is subject to the Act.

(c) Complies with regulations that implement the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164) as in effect on January 1, 2016, if the person is subject to the Act.

(d) Implements an information security program that includes:

(A) Administrative safeguards such as:

(i) Designating one or more employees to coordinate the security program;

(ii) Identifying reasonably foreseeable internal and external risks;

(iii) Assessing whether existing safeguards adequately control the identified risks;

(iv) Training and managing employees in security program practices and procedures;

(v) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring the service providers by contract to maintain the safeguards; and

(vi) Adjusting the security program in light of business changes or new circumstances;

(B) Technical safeguards such as:

(i) Assessing risks in network and software design;

(ii) Assessing risks in information processing, transmission and storage;

(iii) Detecting, preventing and responding to attacks or system failures; and

(iv) Testing and monitoring regularly the effectiveness of key controls, systems and procedures; and

(C) Physical safeguards such as:

(i) Assessing risks of information storage and disposal;

(ii) Detecting, preventing and responding to intrusions;

(iii) Protecting against unauthorized access to or use of personal information during or after collecting, transporting, destroying or disposing of the personal information; and

(iv) Disposing of personal information after the person no longer needs the personal information for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.

(3) A person complies with subsection (2)(d)(C)(iv) of this section if the person contracts with another person engaged in the business of record destruction to dispose of personal information in a manner that is consistent with subsection (2)(d)(C)(iv) of this section.

(4) Notwithstanding subsection (2) of this section, a person that is an owner of a small business as defined in ORS 285B.123 (2) complies with subsection (1) of this section if the person's information security and disposal program contains administrative, technical and physical safeguards and disposal measures that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers. [2007 c.759 §12; 2015 c.357 §3]