554G.2 Affirmative defenses.

1. A covered entity seeking an affirmative defense under this chapter shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of both personal information and restricted information.

2. A covered entity's cybersecurity program shall be designed to do all of the following:

a. Continually evaluate and mitigate any reasonably anticipated internal or external threats or hazards that could lead to a data breach.

b. Periodically evaluate no less than annually the maximum probable loss attainable from a data breach.

c. Communicate to any affected parties the extent of any risk posed and any actions the affected parties could take to reduce any damages if a data breach is known to have occurred.

3. The scale and scope of a covered entity's cybersecurity program is appropriate if the cost to operate the cybersecurity program is no less than the covered entity's most recently calculated maximum probable loss value.

4. *a.* A covered entity that satisfies all requirements of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.

b. A covered entity satisfies all requirements of this section if its cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework, as described in section 554G.3.

2023 Acts, ch 63, §2
Referred to in §554G.3