507F.6 Cybersecurity event — investigation.

1. If a licensee discovers that a cybersecurity event has occurred, or that a cybersecurity event may have occurred, the licensee, or the outside vendor or third-party service provider the licensee has designated to act on behalf of the licensee, shall conduct a prompt investigation of the event.

2. During the investigation, the licensee, outside vendor, or third-party service provider the licensee has designated to act on behalf of the licensee, shall, at a minimum, determine as much of the following as possible:

a. Confirm that a cybersecurity event has occurred.

b. Assess the nature and scope of the cybersecurity event.

c. Identify all nonpublic information that may have been compromised by the cybersecurity event.

d. Perform or oversee reasonable measures to restore the security of any compromised information systems in order to prevent further unauthorized acquisition, release, or use of nonpublic information that is in the licensee's possession, custody, or control.

3. If a licensee learns that a cybersecurity event has occurred, or may have occurred, in an information system maintained by a third-party service provider of the licensee, the licensee shall complete an investigation in compliance with this section, or confirm and document that the third-party service provider has completed an investigation in compliance with this section.

4. A licensee shall maintain all records and documentation related to the licensee's investigation of a cybersecurity event for a minimum of five years from the date of the event, and shall produce the records and documentation upon demand of the commissioner.

2021 Acts, ch 79, §6, 17
Referred to in §507F.9