60A.9852 INVESTIGATION OF A CYBERSECURITY EVENT.

Subdivision 1. **Prompt investigation.** If the licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

Subd. 2. **Investigation contents.** During the investigation, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall, at a minimum and to the extent possible:

(1) determine whether a cybersecurity event has occurred;

(2) assess the nature and scope of the cybersecurity event, if any;

(3) identify whether any nonpublic information was involved in the cybersecurity event and, if so, what nonpublic information was involved; and

(4) perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

Subd. 3. **Third-party systems.** If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee will complete the steps listed in subdivision 2 or confirm and document that the third-party service provider has completed those steps.

Subd. 4. **Records.** The licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and shall produce those records upon demand of the commissioner.

History: *1Sp2021 c 4 art 3 s 7*