304.3-758 Cybersecurity event investigation.

(1) (a) If a 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.

(b) During an investigation required under this subsection, the licensee, or outside vendor or service provider designated to act on behalf of the licensee, shall, at a minimum:

1. Determine whether a cybersecurity event has occurred;
2. Assess the nature and scope of the cybersecurity event;
3. Identify any nonpublic information that may have been involved in the cybersecurity event; 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.

(2) If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall complete, or confirm and document that the third-party service provider has completed, the steps listed in subsection (1)(b) of this section.

(3) Each licensee shall maintain, and produce upon demand of the commissioner, records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event.

Effective: January 1, 2023

History: Created 2022 Ky. Acts ch. 149, sec. 5, effective January 1, 2023.