Ohio Revised Code

Section 3965.03 Investigation of events.

Effective: March 20, 2019
Legislation: Senate Bill 273 - 132nd General Assembly

(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 the investigation, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall, at a minimum, do as much of the following as possible:

(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;

(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.

(C) 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 shall take the actions described in division (B) of this section or make reasonable efforts to confirm and document that the third-party service provider has taken those actions.

(D) 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 superintendent of insurance.