

S.C. Code Ann. § 38-99-30

This document is current through 2024 Regular Session Act No. 120, not including changes and corrections made by the Code Commissioner.

South Carolina Code of Laws Annotated by LexisNexis® > Title 38. Insurance (Chs. 1 — 101) > Chapter 99. South Carolina Insurance Data Security Act (§§ 38-99-10 — 38-99-100)

§ 38-99-30. Investigation of cybersecurity event.

(A) If a licensee learns that a cybersecurity event has occurred or may have occurred, the licensee, an outside vendor, or service provider designated to act on behalf of the licensee must conduct a prompt investigation of the event.

(B) During the investigation, the licensee, outside vendor, or service provider designated to act on behalf of the licensee shall, at a minimum:

- (1) determine whether a cybersecurity event occurred;
- (2) assess the nature and scope of the cybersecurity event;
- (3) identify 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.

(C) If the licensee learns that a cybersecurity event has occurred or may have occurred in a system maintained by a third-party service provider, the licensee shall complete an investigation pursuant to the requirements of this section or confirm and document that the third-party service provider has completed an investigation pursuant to the requirements of this section.

(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 produce those records upon demand of the director.

History

2018 Act No. 171, § 3, effective January 1, 2019.

End of Document