PUBLIC PROTECTION CABINET
Department of Insurance
Financial Standards and Examinations Division
(Amended at ARRS Committee)

806 KAR 3:250. Cybersecurity reporting procedures.

RELATES TO: KRS 304.3-750 – 304.3-768, 45 C.F.R. 160, 164, 15 U.S.C. 6801, 6805
STATUTORY AUTHORITY: KRS 304.2-110, 304.3-756. 304.3-760, 304.3-766
NECESSITY, FUNCTION, AND CONFORMITY: KRS 304.2-110(1) authorizes the Commissioner of the Department of Insurance to promulgate administrative regulations necessary for or as an aid to the effectuation of any provision of the Kentucky Insurance Code. KRS 304.3-756 requires a non-exempt licensee to develop, implement, and maintain a comprehensive information security program based on an internal risk assessment. KRS 304.3-760 and 304.3-766 require non-exempt licensees to notify the Commissioner of the Department of Insurance of a cybersecurity event involving nonpublic information. This administrative regulation establishes the reporting procedures for non-exempt licensees to report a cybersecurity event and file a cybersecurity compliance report. The administrative regulation also establishes the procedure for a licensee to file a cybersecurity exemption form under KRS 304.3-752 and 304.3-766.

Section 1. Definitions.
(1) "Cybersecurity Event" is defined by KRS 304.3-750(2).
(2) "Information security program" is defined by KRS 304.3-750(4).
(3) "Licensee" is defined by KRS 304.3-750(6).
(4) "eServices" means a secured electronic database developed and managed by the Department of Insurance that houses a registration of public and nonpublic information of licensees.

Section 2. Compliance and Exemption Reporting.
(1) A licensee who is domiciled in this state and is not exempt from the requirements of KRS 304.3-750 through KRS 304.3-768 pursuant to KRS 304.3-752, or deemed in compliance with KRS 304.3-750 through 304.3-768 pursuant to KRS 304.3-766, shall file a Cybersecurity Compliance Attestation Form with the department by February 15th of each year, attesting that the licensee has conducted all necessary risk assessments to fully develop an information security program and is currently implementing and executing that information security program as established in KRS 304.3-756.
(2) A licensee who is deemed compliant under KRS 304.3-766, shall file a Cybersecurity Exemption Compliance Form with the department by February 15th of each year, attesting to their compliance with the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. Parts 160 and 164, or the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. 6801 and 6805.
(3) The Cybersecurity Compliance Attestation Form and the Cybersecurity Exemption Compliance Form shall be filed electronically through the licensees' eServices account on the department's secure Web site: https://insurance.ky.gov/doieservices/UserRole.aspx.

Section 3. Reporting a Cybersecurity Event.
(1) If a licensee who is domiciled in Kentucky and is not exempt under KRS 304.3-752, reasonably believes that a cybersecurity event has occurred that meets a qualification established in KRS 304.3-760(1)(a) or (b), the licensee shall:
(a) Report to the commissioner the details of a cybersecurity event within three (3) business days from the determination that a cybersecurity event has occurred; and

(b) Report the cybersecurity event on the Cybersecurity Event Reporting Form submitted electronically through the licensees' eServices account located on the department's secure Web site: https://insurance.ky.gov/doieservices/UserRole.aspx.

(2) A licensee who is not domiciled in Kentucky and who is not exempt as established in KRS 304.3-752, but reasonably believes that the cybersecurity event meets any of the qualifications established in KRS 304.3-760(1)(c), shall:

(a) Report to the commissioner the details of a cybersecurity event within three (3) business days from the determination that a cybersecurity event has occurred; and

(b) Report the cybersecurity event on the Cybersecurity Event Reporting Form submitted electronically through the licensees' eServices account located on the department's secure Web site: https://insurance.ky.gov/doieservices/UserRole.aspx.

(3) A licensee who is deemed compliant under KRS 304.3-766 shall:

(a) Notify the commissioner of a cybersecurity event in the same manner and form no later than the licensee notifies the affected consumers or federal regulatory authorities, as applicable; and

(b) Submit the notification electronically to the commissioner via email at DOI.CommissionerOffice@ky.gov.

Section 4. Amending a Cybersecurity Event Submission. A licensee, who has filed a Cybersecurity Event Reporting Form with the department shall:

(1) Within three (3) business days of the discovery of new information, update and supplement any initial and subsequent cybersecurity event notifications to the commissioner; and

(2) Amend a previously submitted Cybersecurity Event Reporting Form electronically through the licensees' eServices account located on the department's secure Web site: https://insurance.ky.gov/doieservices/UserRole.aspx.

Section 5. Incorporated by Reference.

(1) The following material is incorporated by reference.

(a) "Cybersecurity Compliance Attestation Form", 12/22;

(b) "Cybersecurity Exemption Compliance Form", 12/22; and

(c) "Cybersecurity Event Reporting Form", 12/22.

(2) This material may be inspected, copied, or obtained, subject to applicable copyright law, at the Kentucky Department of Insurance, The Mayo-Underwood Building, 500 Mero Street, Frankfort, Kentucky 40601, Monday through Friday, 8 a.m. to 4:30 p.m. Forms may also be obtained on the Department of Insurance Internet Web site, https://insurance.ky.gov/ppc/CHAPTER.aspx.

(49 Ky.R. 1549, 1942; eff. 7-5-2023.)

FILED WITH LRC: March 7, 2023

CONTACT PERSON: Abigail Gall, Executive Advisor, 500 Mero Street, Frankfort, Kentucky 40601, phone +1 (502) 564-6026, fax +1 (502) 564-1453, email abigail.gall@ky.gov.