Ohio Revised Code

Section 1354.02 Safe harbor requirements.

Effective: November 2, 2018
Legislation: Senate Bill 220 - 132nd General Assembly

(A) A covered entity seeking an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code shall do one of the following:

(1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code; or

(2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code.

(B) A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in division (A)(1) or (2) of this section, as applicable :

(1) Protect the security and confidentiality of the information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

(C) The scale and scope of a covered entity's cybersecurity program under division (A) (1) or (2) of this section, as applicable, is appropriate if it is based on all of the following factors:

(1) The size and complexity of the covered entity;

(2) The nature and scope of the activities of the covered entity;

(3) The sensitivity of the information to be protected;

(4) The cost and availability of tools to improve information security and reduce vulnerabilities;

(5) The resources available to the covered entity.

(D)(1) A covered entity that satisfies divisions (A)(1), (B), and (C) of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information.

(2) A covered entity that satisfies divisions (A)(2), (B), and (C) of this section is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.