Ohio Administrative Code

Rule 3357:15-16-15 Cybersecurity policy.

Effective: February 14, 2020

(A) Purpose: To meet each requirement for the minimal risk profile in the cybersecurity assessment tool (CAT) of the federal financial institutions examination council (FFIEC), to comply with the information technology examination handbook (IT handbook) and the national institute of standards and technology (NIST) cybersecurity framework, and to continue to increase cybersecurity maturity from baseline to evolving and beyond, as those terms are described in the instructions of the CAT.

(B) Authority: C.F.R. Title 16 Chapter I Subchapter C Part 314, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(C) Scope: The college shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to our size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue. The information security program shall include the administrative, technical, or physical safeguards the college uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. Such safeguards shall include the elements set forth in paragraph (D) of this rule and shall be reasonably designed to achieve the following objectives:

(1) Insure the security and confidentiality of customer information;

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

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

(D) Program: The college shall develop, implement, and maintain its information security program in the following manner:

(1) Designations: The college designates its vice president for business, finance and information technology or his or her qualified designee to lead the cybersecurity coordinating committee, including the director of information technology and the director of financial aid to coordinate the colleges information security program.

(2) Assessments: The cybersecurity coordinating committee will identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of college operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(c) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(3) The cybersecurity coordinating committee will ensure that the college designs and implements information safeguards to control the risks it has identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(4) The cybersecurity coordinating committee will oversee service providers, by:

(a) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(b) Requiring the colleges service providers by contract to implement and maintain such safeguards.

(5) The cybersecurity coordinating committee will evaluate and adjust the colleges information security program in light of the results of the testing and monitoring required by paragraph (D)(3) of this rule; any material changes to college operations or business arrangements; or any other circumstances that the college knows or has reason to know may have a material impact on its information security program.

(E) Public records: Procedures shall be documented and utilized by the college. To the extent such documentation meets the definition of security record or infrastructure record as identified by division (B)(1) of section 149.433 of the Revised Code, those records shall not be public records and shall not be subject to release or inspection by the public.