3359-11-10.4 Customer information security policy.

(A) Introduction.

(1) The university of Akron is committed to respecting and protecting the privacy of non-public customer information. The purpose of the policy outlined in this document is to enable appropriate university officials to implement a comprehensive written information security program and comply with the provisions of the federal trade commission's safeguard rules implementing applicable provisions of the Gramm-Leach-Bliley Act.

(2) This policy incorporates by reference the institution's policies and procedures found in rule 3359-11-08 of the Administrative Code related to policies and procedure for student records and rule 3359-11-10.3 of the Administrative Code related to information technology security and system integrity, and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including but not limited to the Family Educational Rights and Privacy Act.

(B) Scope. This policy and its corresponding comprehensive written information security program apply to any record containing non-public financial information about a customer who has a relationship with the university, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the university or its affiliates.

(C) Definitions

(1) Customer. A customer is any individual who receives a financial service from the university and who, in the course of receiving that financial service, provides the university with non-public financial information about themselves. Customers may include, but are not limited to, students, parents, faculty, staff and other third parties with whom the university interacts.

(2) Customer information. Customer information means any non-public financial information about a customer that is handled or maintained by or on behalf of the university or its affiliates.

(3) Non-public financial information. Non-public financial information means any information:

(a) A customer provides in order to obtain a financial service from the university;

(b) About a customer resulting from any transaction with the university involving a financial service;

(c) Otherwise obtained about a customer in connection with providing a financial service to that customer; or

(d) Any list, description or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available.

(D) Information security program coordinator.

(1) The president shall appoint an information security program coordinator to implement, coordinate and oversee the information security program at the university of Akron. The "ISPC" shall seek to assure that customer information is secure at the university and shall be responsible for the following duties:

(a) Designing and implementing, with the assistance of the university's information technology security officer ("ITSO"), appropriate individuals in the affected offices of the university and any other individuals the "ISPC" deems appropriate, safeguards, systems, procedures and protocols, which, together with this rule, shall comprise the university's comprehensive written information security program;

(b) Assisting the "ITSO," human resources and the relevant offices of the university in identifying 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, by considering the following factors:

(i) Employee training and management;

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

(iii) The university's ability to detect, prevent and respond to attacks, intrusions or other system failures.

(c) Assessing the effectiveness of the current safeguards, systems and procedures for controlling identified risks to the security, confidentiality and integrity of customer information;

(d) Designing and implementing additional information safeguards, systems or procedures necessary to control identified risks to the security, confidentiality and integrity of customer information;

(e) Monitoring and testing the effectiveness of customer information safeguards, systems and procedures at regular intervals;

(f) Coordinating with those responsible for third party service procurement activities for affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for customer information to which they will have access;

(g) Evaluating and revising the university's comprehensive written information security program in light of the results of the testing and monitoring of the university's comprehensive written information security program, any material changes to the university's operations or business arrangements or any other circumstances that the "ISPC" knows or has reason to know may have a material impact on the university's information security program;

(h) Coordinating with the "ITSO" and appropriate individuals in the relevant offices of the university to respond to perceived breaches of the security of customer information, if such breach should occur; and

(i) Coordinating with the office of general counsel, human resources and the "ITSO" to provide training regarding customer information security practices and procedures to faculty, staff and students as the "ISPC" deems necessary.

(E) Service Providers.

(1) The university shall only select and retain service providers that are capable of maintaining appropriate safeguards for the customer information to which they will have access.

(2) The university shall require, by contract, service providers who have access to customer information to implement and maintain appropriate safeguards for that customer information.

(3) Any deviation from the service provider requirement shall require the office of general counsel's prior approval.

(4) The service provider requirements shall apply to all existing and future

contracts entered into with third party service providers who have access to customer information, provided that amendments to contracts entered into prior to June 24, 2002 are not required to be effective until May 2004.

(F) Compliance.

(1) All university personnel shall cooperate fully with the university "ISPC."

Replaces:	3359-11-10.4
Effective:	01/31/2015
Certification:	_____ Ted A. Mallo Secretary Board of Trustees
Promulgated Under:	111.15
Statutory Authority:	3359.01
Rule Amplifies:	3359.01
Prior Effective Dates:	06/09/03, 06/25/07