Michigan State University Customer Information Security Program

Updated: 5-June-2018

Michigan State University (MSU) has adopted a Customer Information Security Program (CISP) in compliance with the Safeguards Rule issued by the Federal Trade Commission pursuant to the Gramm-Leach-Bliley Act (GLB). Units within the University that are "significantly engaged" in providing financial products or services to customers are subject to this CISP.

Background

The Safeguards Rule requires MSU units that are significantly engaged in providing financial products or services to safeguard the confidentiality and security of its customers' nonpublic personal information. Data safeguarding has two major components: privacy and security.

MSU is deemed to be in compliance with the privacy provisions of the GLB when it is in compliance with the Family Education Rights and Privacy Act (FERPA). However, MSU is subject to the provisions of GLB related to the security of customer information.

Compliance Coordinator

The Controller's Office (CO) coordinates MSU compliance with the Safeguards Rule and this CISP. CO will:

- Assist in identification of MSU units that are subject to this CISP;
- Advise each unit that is subject to the Safeguards Rule of its responsibility to design a unit security program (Unit CISP);
- Advise each unit of its responsibility to identify and formally assess risks to customer information and to evaluate the effectiveness of the current safeguards for controlling such risk, at least annually; and
- Advise each affected unit to evaluate and modify its Unit CISP and formal risk assessment document in light of relevant circumstances, including changes in operations, the results of security testing and monitoring, or findings of internal or external auditors.
- Manage the central depository for university-level GLB documentation.
- Regularly maintain and update this document.

CO retains a copy of each Unit's CISP as well as the MSU CISP document. Unit Risk Assessment documents are maintained by and retained within the affected unit.

Unit Requirements

Each MSU unit that is significantly engaged in providing financial products or services, or providing services to hold customer data, shall appoint a person to coordinate security implementation, incident response, and periodic user access reviews. This unit contact:

- Develops or coordinates development of a written Unit CISP and forwards a copy to CO.
- Develops or coordinates development of a formal Risk Assessment document within the unit which explores and proposes solutions for privacy and safeguarding vulnerabilities. Each unit should consider the following non-exhaustive areas when assessing risk:

    - Employee Training and Management – train staff how to release or update information appropriately;
    - Information Systems – network and software design, information processing, data storage and transmission, access management, and proper/secure retrieval and disposal of data (paper and electronic);
    - Detecting and Managing System Failures – written contingency plan that addresses the detection and response to security breaches, software patches to address vulnerabilities, use of anti-virus software, monitor system access, disaster recovery plans.
- Ensures a formal Risk Assessment is performed on a regular basis.
- Facilitates practices that secure customer information in accordance with the Unit CISP's specifications.
- Require service providers, through contract language, to maintain appropriate security of customer information. (See Exhibits A).

Each unit must instruct its employees to maintain confidentiality of customer information. It is recommended that staff receive refresher training on the Safeguards Rule requirements on a regular basis.

Evaluation of Safeguards and Adjustments to Program

The MSU CISP shall be evaluated and adjusted as circumstances dictate. Events, if deemed significant and relevant that might trigger a review of this document, supporting documents, and relevant practices include:

- Changes in regulatory requirements
- Changes in University business arrangements and operations
- Changes resulting from Internal Audit recommendations
- Changes resulting from testing and monitoring of the safeguards

Risk assessment will be done on a continuing basis by relevant MSU departments utilizing industry risk assessment standards and available tools.

The Controller's Office and/or the Office of General Counsel should be contacted to evaluate new or changed business arrangements to be considered for inclusion in this CISP.

The Controller's Office will convene a committee of the responsible offices to perform a regular review of the CISP.

References:

Federal Trade Commission: Standards for Safeguarding Customer Information: Final Rule