Policy Number: 246.0
Policy: Safeguarding Customer Information
Effective Date: 3/2013
Revision Date: 7/2017
Approved by: Business Services Director

POLICY:

Safeguarding Customer Information:

A. Introduction and Purpose:

This policy is being introduced as required by the Federal Trade Commission under the Gramm-Leach Bliley (GLB) Act and the Payment Card Industry Data Security Standards.

At Montana State University - Billings, safeguarding the privacy and confidentiality of personal information is important. As an institution of higher education, we collect, retain, and use personal non-public information about individual students and staff members. We may collect personal information from such sources as hard copy applications, electronic forms, background checks, or over the Internet. The objectives of our information security program are to ensure the security and confidentiality of such personal information; to protect against any anticipated threats to its security or integrity; and to guard it against unauthorized access to or use.

Any sharing of nonpublic personal information about our students or employees must be done in strict adherence to the Federal Family Educational Rights and Privacy Act (FERPA) guidelines. The University may exchange such information with certain nonaffiliated third parties (under limited circumstances) to the extent permissible under law. Examples may include (but are not limited to) medical insurance institutions or credit card processing software companies.

We restrict access to student and employee information only to those employees who have business reasons to know such information, and we educate our employees and contract service providers about the importance of confidentiality and privacy.

B. Policy:

1. In order to provide adequate safeguards over customers' credit card data and electronic addresses as they are received over the Web, the university will adhere to the following minimum technical specifications:

    a. Any computer device on the University network that makes non-personal public information available must be certified secure. A copy of the security certificate must be completed with IT before any such computing device that is connected to the network.

b. Customer information, including credit card data, must be reasonably secured against disclosure and modification as determined by current campus policy.

c. The University must oversee local and contracted service providers by taking steps to select and retain providers that are proven capable of maintaining appropriate safeguards for customer information and PCI-DSS compliant.

d. MSU Billings will contractually require service providers to implement and maintain such safeguards; and

e. MSU Billings will periodically evaluate, based on results of testing and monitoring, any material changes to the service providers' operations.

2. Departments may develop Web pages to accept payment by credit card under the following circumstances:

   a. The department must complete the application for Authorization to Process Bankcard Transactions to apply to become an authorized merchant department and return it to University Business Services. (Request MSU startup procedures for processing credit cards from University Business Services). Procedures for timely deposit of credit card transactions and safe and proper handling of the data must be followed.

   b. The department must also complete the application for Authorization to Process Bankcard Transactions Over the Internet, requesting approval from University Business Services, Institutional Audit & Advisory Services, and UIT before the Web page is approved to be put into production.

3. IT will review the department's hardware and software to ensure that the server is secure and the program requirements have been adhered to. (See Procedures). Internal Audit will review the department's internal procedures to ensure that personal information is handled utilizing reasonable confidentiality security practices.

4. The following safeguards need to be in place:

   a. Personal computers containing confidential information must be secure.

   b. Adequate internal controls regarding separation of duties must be in place.

   c. It is the merchant department's responsibility to maintain the customer's credit card or e-mail information in a confidential manner as shown in PCI-DSS Procedures Departmental Agreement Form.

   d. Any hard copy documents containing confidential information must be shredded in a timely manner.

   e. The merchant department must follow the MSU Billings Business Procedures Manual regarding procedures for safe handling of money deposits.