

Policy:	
Title:	Information and Data Protection
Effective:	
Senate Proposal:	No
Responsible University Officer:	Vice President Governmental Relations
Responsible Office:	Governmental Relations

Policy Statement

The University will provide safeguards to protect information and data in compliance with The Financial Services Modernization Act of 1999, also known as Gramm Leach Bliley (GLB) 15 U.S.C. §6801, and in compliance with other federal and state laws related to privacy and protection of personal information.

Policy Requirements

The information and data safeguards will provide:

- *Security and confidentiality of Protected Information;
- *Protection against anticipated threats or hazards to the security or integrity of such information; and
- *Protection against unauthorized access to or use of Protected Information that could result in substantial harm or inconvenience to any customer.

Gramm Leach Bliley (GLB) mandates that the University:

- *Appoint an Information Security Plan Coordinator
- *Conduct a risk assessment of likely security and privacy risks
- *Institute a training program for all employees who have access to covered data and information
- *Oversee service providers and contracts
- *Evaluate and adjust the Information Security Program periodically.

Reason for Policy

This policy was developed pursuant to Gramm Leach Bliley (GLB) requirements, a federal law. The statute was enacted November 12, 1999 with the Regulations effective date November 13, 2000 and a compliance date of July 1, 2001.

Related Policy Information

The Gramm Leach Bliley Act Oversight Committee developed the MTU Information Security Plan with recommendations suggested by various departments and divisions.

Exclusions

Contact(s)

<u>Office/Unit</u>	<u>Telephone Number</u>
Vice President Governmental Relations	7-2318
Information Technology, Senior Security Officer	7-1727

Definitions

Protected data and information - All student information, credit card information received in the course of business by the university, personnel files, and financial records. Protected data and information includes both paper and electronic records.

Responsibilities

Information Security Policy Coordinator - Works closely with the University Counsel's office, the Networking and Security Administrator in Information Technology, other positions in Information Technology, as well as all relevant academic and administrative departments throughout the University to identify potential and actual internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program. Periodically reviews the University's disaster recovery program and data-retention policies and prepares a report for the Executive Team. The Coordinator is presently the Information Technology Senior Security Officer.

Information Technology Department - Assigns appropriate GLBA responsibilities to a staff member.

Directors/Chairs/Deans or designee - Conducts an annual data security review with guidance from the Coordinator.

Executive Team - Identifies any employees in their respective areas that work with protected data and information.

Procedures

In support of this policy, the following procedures are included:

Forms and Instructions

In support of this policy, the following forms/instructions are included:

Appendices

Appendix A - MTU Information Security Plan

<http://www.admin.mtu.edu/acct/dept/controller/glba/DRAFTappA.pdf>

Appendix B - Risk Assessment

<http://www.admin.mtu.edu/acct/dept/controller/glba/glbaRA.pdf>

Additional Information

To view the entire Gramm Leach Bliley (GLB) Act, refer to;

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

History

Adoption Date: