

## Appendix A - MTU Information Security Plan

### I. Preamble

In order to protect critical information and data, and to comply with Federal Law , Information Technology Services (ITS), in alliance with the University Counsel (UC) proposes certain practices in the University information environment and institutional information security procedures. While these practices mostly affect ITS, some of them will impact diverse areas of the University, including but not limited to Accounting Services (including Student billing), the Office of Student Records and Registration, Student Life, the Financial Aid Office, and many third party contractors. The goal of this document is to define the University's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the University for likely future privacy and security regulations.

### II. Gramm Leach Bliley (GLB) Requirements

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, and evaluate and adjust the Information Security Program periodically.

### III. Information Security Plan Coordinator

In order to comply with GLB, the University has designated an Information Security Policy Coordinator. This individual will work closely with the University Counsel's office, the Services Networking and Security Administrator in Information Technology, other positions in Information Technology, as well as all relevant academic and administrative departments throughout the University. The Coordinator is presently the Information Technology Services Senior Security Officer.

The Coordinator must help the relevant offices of the University identify reasonably foreseeable 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.

### IV. Risk Assessment and Safeguards

The Coordinator must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. Each Dean or Director, or designee, will conduct an annual data security review with guidance from the Coordinator. The Executive Team will be asked to identify any

employees in their respective areas that work with covered data and information. ITS bears primary responsibility for the identification of internal and external risk assessment, but all members of the University community are involved in risk assessment. ITS, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB. ITS will assure the physical security of all servers and terminals which contain or have access to protected data and information. ITS will work with other relevant areas of the university to develop guidelines for physical security of any covered servers in locations outside the central server area.

ITS will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

ITS will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

#### V. Employee training and education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, ITS and the UC will work in cooperation with the Office of Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all university data; custodians of data, and those employees who use the data as part of their essential job duties.

#### VI. Oversight of Service Providers and Contracts

GLB requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Accounting Services, in cooperation with the University Counsel, will develop and send form letters to all covered contractors requesting assurances of GLB compliance. The University Counsel will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.