BOARD OF REGENTS
EASTERN MICHIGAN UNIVERSITY

SECTION: 29
DATE: June 19, 2012

RECOMMENDATION

The Gramm Leach Bliley Act

ACTION REQUESTED

It is recommended that the Board of Regents adopt the attached policy establishing an Identity Theft Prevention Program at the University as required by Federal Law (Gramm-Leach-Bliley Act).

STAFF SUMMARY

Eastern Michigan University is considered to be a financial institution by the Federal Trade Commission (FTC) and as a result is required to adopt policies and procedures to comply with the Privacy and Safeguards Rules of the Gramm Leach Bliley Act (GLBA).

The Gramm Leach Bliley Act is a comprehensive federal law requiring all financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information.

FISCAL IMPLICATIONS

None

ADMINISTRATIVE RECOMMENDATION

The proposed action has been reviewed and is recommended for Board approval.

University Executive Officer **Date**

BOARD OF REGENTS
EASTERN MICHIGAN UNIVERSITY

Effective Date: June 19, 2012
Policy: Gramm-Leach-Bliley Act

BACKGROUND:
Institutions of higher education are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA) Act for the purposes of this information safeguarding policy. Subtitle A of Title V of the Act limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose certain privacy policies and practices with respect to its information sharing with both affiliates and nonaffiliated third parties. Institutions of Higher Education are generally exempt from the notice provision because they already do so under the Federal Educational Rights and Privacy Act (FERPA).

UNIVERSITY STATEMENT:
The statutory and regulatory standards under GLBA are intended to "ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer". The University shall implement and maintain a written information security program that establishes the appropriate administrative, technical, and physical safeguards. In order to accomplish these objectives, GLBA requires the following:

- Designate one or more employees to coordinate the Information Security Program
- Assess risks to the security of customer information
- Design and implement safeguards to address risks, and test and monitor their effectiveness over time
- Adjust the program to address developments
- Employee training and oversight of service providers

RESPONSIBILITY AND IMPLEMENTATION:
Provost and Vice President, Chief Financial Officer, and Chief Information Officer

SCOPE OF POLICY COVERAGE:
All University employees that handle or have access to nonpublic personal information or oversee service providers with whom we share nonpublic personal information