COLLEGE OF MICRONESIA-FSM

BOARD POLICY No. 8930

Gramm-Leach-Bliley Act (GLBA) Compliance Policy

Date Adopted:

Date Revised:

Date Reviewed:

References:	Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801-6809, Federal Trade Commission (FTC) Safeguards Rule, 16 CFR Part 314, U.S. Department of Education, Federal Student Aid Handbook (Volume 2, Chapter 6 – "Safeguarding Student Information"), U.S. Department of Education Cybersecurity Compliance and GLBA Audit Guide, Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99

Purpose

The College of Micronesia-FSM is committed to protecting the privacy and security of nonpublic personal information (NPI) as required under the Gramm-Leach-Bliley Act (GLBA). This policy outlines the College's commitment to implementing administrative, technical, and physical safeguards to protect such information.

Scope

This policy applies to all employees, contractors, service providers, and departments that access, manage, or store NPI collected for student financial aid or other covered services.

Policy Statement

The College shall develop, implement, and maintain a comprehensive Written Information Security Program (WISP) designed to:

- Protect the security, confidentiality, and integrity of customer information;
- Identify and assess internal and external risks to information systems;
- Provide safeguards to control identified risks;
- Regularly monitor, test, and adjust security controls;
- Oversee service providers to ensure they also comply with GLBA standards;
- Respond appropriately to security incidents and data breaches;
- Train employees to recognize and properly handle sensitive information.

Governance

The Director of Information Technology (DIT) is designated as the Information Security Program Coordinator and is responsible for overseeing the implementation, maintenance, and review of the GLBA compliance program.

Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, as well as potential civil or criminal penalties as allowed by law.

Review and Revision

This policy will be reviewed regularly or as needed in response to changes in regulatory, operational, or technological requirements.

See Administrative Procedure 8930