COLLEGE OF MICRONESIA-FSM

ADMINISTRATIVE PROCEDURE No. 8930

Gramm-Leach-Bliley Act (GLBA) Compliance Policy

Date Adopted:	11 June 2025
Date Revised:	11 June 2025
Date Reviewed:	11 June 2025
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

To establish administrative procedures for implementing and maintaining the Written Information Security Program (WISP) in accordance with the Gramm-Leach-Bliley Act (GLBA) and FTC Safeguards Rule.

Definitions

- Nonpublic Personal Information (NPI): Any personally identifiable financial information not publicly available (e.g., Social Security numbers, loan data).
- Service Provider: Any third party with access to NPI while delivering services on behalf of the College.
- WISP: Written Information Security Program.
- Information Security Program Coordinator: Designated by the Vice President, Institutional Effectiveness and Quality Assurance (IEQA); typically the Director Information Technology (DIT).

Responsibilities

- Director Information Technology (DIT):
    - Serves as the Information Security Program Coordinator.
    - Leads implementation of the WISP and ensures ongoing compliance.
    - Coordinates risk assessments and training programs.

Information Technology Committee (ICT):

- Advises the DIT.
- Reviews risk findings and recommends improvements.

- Includes representatives from IT, Financial Aid, Registrar, Business Office, and HR.

Data Owners (e.g., Director of Financial Aid, Registrar, Comptroller):

- Classify and manage access to data under their authority.
- Ensure compliance within their areas.

IT Staff (Data Custodians):

- Implement technical safeguards.
- Manage secure infrastructure and monitor systems.

Risk Assessment

- Conducted annually to identify and assess internal/external threats to NPI.
- Includes areas such as:
  - Employee practices and training
  - IT systems (network, servers, applications)
  - Physical security
  - Data retention and disposal practices
- Documented in a formal report and reviewed by the ICT.

Safeguards and Security Controls

- Access to NPI is granted based on the principle of least privilege.
- Multi-factor authentication (MFA) is required for all remote and administrative access.
- All data containing NPI is encrypted during storage and transmission (AES-256, TLS 1.2+).
- Electronic and physical media must be disposed of securely (e.g., shredding, data wiping).
- Systems are updated and patched regularly.

Employee Training

- All employees with access to NPI must complete annual training on GLBA, cybersecurity, and breach response.
- New employees must complete training within 30 days of hiring.
- HR maintains training records.

Vendor and Service Provider Oversight

- Contracts must include GLBA compliance requirements.
- All vendors with NPI access must undergo:
  - Initial and annual security assessments
  - Independent audits for high-risk vendors every two years
- Vendor security reviews are documented and stored by the DIT.

Incident Response

- Suspected or actual data breaches must be reported immediately to the DIT.
- The Incident Response Plan outlines steps for containment, investigation, notification, and recovery.
- Periodic tabletop exercises are conducted.

Business Continuity

- Business Continuity and Disaster Recovery Plans must account for systems containing NPI.
- Plans are reviewed and tested annually.

Monitoring and Evaluation

- Security controls are subject to:
  - Regular audits and vulnerability scans
  - Penetration testing as needed
- Key metrics are tracked (e.g., number of incidents, training compliance).
- The WISP and procedures are reviewed annually and updated as necessary.

Compliance and Enforcement

- Non-compliance with this procedure may result in disciplinary action and/or legal consequences.
- All staff are encouraged to report suspected violations or security concerns.

See Board Policy 8930