University of Guam GLBA Written Information Security Program

1. Purpose

The Gramm-Leach-Bliley Act ("GLBA") (Public Law 106-102) and its implementing regulations at 16 CFR Part 313 & 314 requires Financial Institutions to protect, to the extent reasonably possible, the security, privacy, and confidentiality of personally identifiable financial records and information, also known as "Covered Information." Because the University of Guam ("University") engages in Financial Services, such as student financial aid, the Federal Trade Commission ("FTC") considers the University a Financial Institution for GLBA purposes.

This program establishes the University of Guam's commitment to protecting the security, confidentiality, and integrity of nonpublic financial information in compliance with the Gramm-Leach-Bliley Act (GLBA) and the FTC Safeguards Rule (16 CFR Part 314).

2. Scope

This policy applies to all University departments and personnel who access, process, store, or transmit Covered Information, including but not limited to:

- Financial Aid Office

- Bursar's Office

- Office of Information Technology (OIT)

- Third-party service providers

3. Definitions

Covered Information: Nonpublic personal financial information obtained in connection with providing a financial product or service.

Customer Information: Information about students or others who receive financial services from the University.

Qualified Individual: The designated person responsible for implementing and overseeing the Information Security Program (ISP).

Service Provider: Any third party with access to Covered Information through a contractual relationship with the University.

4. Governance

The Chief Information Officer (CIO) is designated as the Qualified Individual responsible for the ISP. The CIO may delegate responsibilities to appropriate personnel within OIT, other departments, and/or a contracted virtual Chief Information Security Officer (VCISO).

5. Program Elements

5.1 Risk Assessment

UOG intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.

The University will:

- Identify internal and external risks to Covered Information
- Assess the effectiveness of current safeguards
- Evaluate risks in areas including:
    - Employee training and management
    - Information systems and data lifecycle
    - Incident detection and response

5.2 Safeguards Implementation

- Implement and periodically review access controls such as Role-based access to systems containing Covered Information.

- Asset inventory - Know what you have and where you have it.

- Encryption: Encrypt data at rest and in transit.

- Multi-Factor Authentication (MFA): Required for all systems accessing Covered Information.

- Secure Disposal: Procedures for securely disposing of paper and electronic records.

- System Monitoring: Logging and monitoring of user activity and system access.

5.3 Employee Training

Annual training for all employees with access to Covered Information, including data handling, phishing awareness, and incident reporting.

5.4 Oversight of Service Providers

- Contracts must require service providers to implement appropriate safeguards.

- The Office of Procurement and Legal Affairs will ensure GLBA compliance in vendor agreements.

- Periodic reviews of vendor compliance will be conducted.

5.5 Incident Response

The University will maintain an incident response plan to detect, respond to, and recover from security incidents. All incidents involving Covered Information must be reported to the CIO and the Office of Information Technology – Information Security Section.

5.6 Program Review and Adjustment

The ISP will be reviewed annually or upon significant changes in operations or threats. Adjustments will be made based on risk assessments, audit findings, and regulatory updates.

6. Enforcement

- Any employee, contractor, or other third-party performing duties on behalf of the University with knowledge of an alleged violation of this Policy shall notify the Office of Information Technology as soon as practicable.
- Any employee, contractor, or other third-party performing duties on behalf of the University who willfully and/or repeatedly violates this Policy may have their access to University Information Resources suspended or revoked. Disciplinary actions for employees will follow the University's standard administrative processes and

applicable policies. For contractors and third-party vendors, remedies will be enforced in accordance with the terms and conditions of their contract, which may include termination of services or other contractual remedies.