Security of Student Information

Gramm Leach Bliley Act Information Safeguards Rule
(Consumer Financial Information Privacy)

disposal of nonpublic financial information. This evaluation will include assessing the Institution's current policies and procedures relating to the Information Technology Acceptable Use Policy, Information Technology Security Policy, and Records Retention Policy. The Program Officer will also assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

Detecting, Preventing and Responding to Attacks. The Program Officer will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the Department of Information Technology the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers. The Program Officer shall coordinate with those responsible for the third-party service procurement activities among the Department of Information Technology and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. Any deviation from these standard provisions will require the approval of the University Attorney. These standards shall apply to all existing and future contracts negotiated with such third-party service providers.

5. Adjustments to Program

The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the tution's

Security of Student Information

Gramm Leach Bliley Act Information Safeguards Rule
(Consumer Financial Information Privacy)

7. Policy Attributes

Responsible Office(s)	Information Technology, 1410 N. Oak St., 229-245-4357, itvsu@valdosta.edu
Approving Officer or Body	President, President's Office, West Hall Suite 1004, 229-333-5952, president@valdosta.edu
Date Approved	05/23/2003
Last Reviewed Date	07/01/2020
Next Review Date	07/01/2022