Policy Owner:	Office of Information Technology
Applicability:	Human Resources, Information Technologies, Business Continuity and Disaster Recovery, Mission Critical Systems and Data Hosted in the Cloud, Enrollment Services, Registration, Financial Aid, Finance, Public Safety
Effective Date:	May 18, 2024

Information Technology Policy – Gramm-Leach Bliley Act

Policy Statement:

In order to protect confidential information and data, and to comply with federal laws, this document summarizes the University's comprehensive written Information Security Program (the "Program"). The Gramm-Leach Bliley Act of 2000 (the "GLBA") mandates that financial institutions must take steps to safeguard the security and confidentiality of customer information. Compliance with the GLBA involves compliance with 1) the privacy provisions of the GLBA and 2) provisions regarding the safeguarding of customer information. The GLBA mandates that the University appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Program periodically.

Scope:

This policy is platform and technology neutral, and applies to the entire University, including the Newport Campus, any and all other affiliates.

Definitions:

1. **Covered data and information.** Covered data and information includes student financial information required to be protected under the GLBA. Covered data and information includes both paper and electronic records.

2. **Student financial information.** Student financial information is that information the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in both paper and electronic format.

3. **Program Coordinator.** The University has designated a Program Coordinator. This individual must work closely with the University's Information Technology and Information Systems and Services, as well as all relevant academic and administrative Departments throughout the

University. The Coordinator is presently the Chief Information Security Officer (CISO). The Coordinator must help the relevant offices of the University identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program; and regularly monitor and test the Program.

4. **Areas Identified.** The following offices have been identified as relevant areas to be considered when assessing the risks to customer information:

   (1) Human Resources
   (2) Information Technology
   (3) Business Continuity and Disaster Recovery
   (4) Mission Critical Systems and Data Hosted in the Cloud
   (5) Enrollment Services
   (6) Registration
   (7) Financial Aid
   (8) Finance
   (9) Public Safety

Goals:

It is the policy of the Salve Regina University to fully comply with the Gramm-Leach Bliley Act of 2000.

General Principles:

Risk Assessment and Safeguards:

The Coordinator must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. Each University or Department head, or his/her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant departments of the will conduct a quarterly review of procedures, incidents, and responses, and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the University community on network security and privacy issues. The University will assure that procedures and responses are appropriately reflective of those widely practiced at other similar institutions.

In order to protect the security and integrity of the University network and its data, the University will develop and maintain a registry of all computers attached to the University network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has or has special access to any confidential data covered by relevant external laws or regulations.

The University bears primary responsibility for the identification of internal and external risk assessment, but all members of the University community are involved in risk assessment. The University, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by the GLBA.

The University, working in cooperation with relevant University departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). The University and the relevant departments will conduct ongoing (at least biannual) audits of activity and will report any significant questionable activities.

The University will work with the relevant offices to develop and maintain a registry of those members of the University community who have access to covered data and information. The University, in cooperation with Human Resources and Business Office, will work to keep this registry rigorously up to date.

The University will assure the physical security of all servers and terminals which contain or have access to covered data and information. The University will work with other relevant areas of the University to develop guidelines for physical security of any covered servers in locations outside the central server area. The University will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the University to risks.

One of the largest security risks may be the possible non-standard practices concerning social security numbers. Social security numbers are considered protected information under both the GLBA and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers remain in the University student information system. The University will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover University employees as well as subcontractors.

The University will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

It is recommended that relevant offices of the University decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees. For example, employees handling confidential financial information.

The University will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

The Program Coordinator will periodically review the University's disaster recovery program and data-retention policies and present a report to the Vice Presidents.

Employee Education and Training:

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the University will work in cooperation with the Office of Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all University data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.

Oversight of Service Providers and Contracts:

The GLBA requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The University's Business Office will develop and send form letters to all covered contractors requesting assurances of GLBA compliance.

Evaluation and Revision of the Program:

The GLBA mandates that the Program be subject to periodic review and adjustment. The most frequent of these reviews will occur where constantly changing technology and constantly evolving risks indicate the wisdom of quarterly reviews. Processes in other relevant offices of the University such as data access procedures and the training program should undergo regular review. The Program itself as well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.