University of Louisville
Gramm-Leach-Bliley Act
Information Security Program

I. Purpose

This document summarizes the University of Louisville's (University) Gramm-Leach-Bliley Act Information Security Program (Program) as mandated by the Federal Trade Commissions' Safeguards Rule and the Gramm-Leach-Bliley Act (GLB) which requires security and confidentiality of customer information collected or maintained by or on behalf of financial institutions or their affiliates. The University is classified as a financial institution under GLB due to processing or servicing student loans or offering other financial products or services. As required by the Safeguards Rule, the Program is designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

II. Definitions

Customer information is defined as any record containing nonpublic, personally identifiable financial information, whether in paper, electronic, or other form, that the University obtains from a student, a student's parent(s) or spouse, employee, alumnus or other third party, in the process of offering a financial product or service; or such information provided to the University by another financial institution; or such information otherwise obtained by the University in connection with providing a financial product or service. Examples include name, address, phone number, bank and credit card account information, income and credit histories, and social security numbers.

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 paper and electronic format.

Covered data and information for the purpose of this program includes student financial information required to be protected under the Gramm-Leach-Bliley Act (GLB). In addition to this coverage, which is required by federal law, the University may choose as a matter of policy to also define *covered data and information* to include personally identifiable financial information obtained during the course of business by the university, whether or not such information is covered by GLB. Covered data and information include both paper and electronic records.

Service Providers refers to all third parties who, in the ordinary course of University business, are provided access to covered data. Service providers may include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers, as example.

III. Scope and Applicability

The University has adopted this Program for certain highly critical and private financial and related information. The Program supports the overall strategic information security program of the University. This program applies to financial information (covered data) the University receives during business as required by GLB as well as other confidential

financial information the University may voluntarily choose as a matter of policy to include within its scope. The program is a continuous process that is reviewed at periodic intervals.

The following table illustrates mapping of the departments and services that the University has determined fall under the scope of the GLB Safeguard Rules. Additional services which may fall outside of the defined scope but deal with personal information and are therefore required to implement security safeguards are also be noted.

Financial services under the GLB Safeguarding Rule	**Departments that provide or initiate financial services**
• Student Loans (federal) • Private Student loans (alternative) • Disbursement of Financial Aid • Payment Plans (tuition, housing, meal and ticket plans) • Collections (Delinquent Loans) • 1098 (Tax docs due to financial aid) Personal Identifiable Information of Students - SSN, Billing Information, Credit Card, Account Balance, Citizenship, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth	• Financial Aid • Bursar • System: Campus Solutions

Other Personal Information services	**Departments that may receive data from financial services or deal with general PI**
• Employee Payroll/W2s/Pay Advances/Garnishments/I-9/Pay deductions • Other – I-9 and other employment doc for temps, lecturers, grads students • Audits 1099s • Information from housing and ticket plans Personal Identifiable Information of Students and Employees - SSN, Billing Information, Credit Card, Account Balance, Citizenship, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth	• Payroll • Business Operations • Human Resources • Controller • Cardinal Card Office • Office of Admission • Office of the Registrar • Athletics

IV. GLB Information Security Program Components

<u>GLB Information Security Program Committee</u>

The Chief Information Security Officer (CISO) is responsible for the university's overall information security program. The GLB Information Security Program Committee (Committee) is responsible for coordinating and overseeing the GLBA Security Program. The Committee is led by the Information Security Compliance Officer (ISCO) and consist of representatives from the Offices of the Bursar, Finance, Student Financial Aid, Information Technology Services (ITS), General Counsel, Risk Management, and Admissions. The Committee will act as a consultant and coordinate Program activities with areas that provide services dealing with information covered under GLB. The Committee may designate

other representatives to oversee and coordinate particular elements of the Program. Program compliance is the responsibility of each covered area.

- The Committee will consult with responsible parties to identify areas covered under GLB, ensure that areas and functions are included within the scope of the Program and maintain a current listing of areas and functions.
- The Committee will ensure covered departments develop appropriate training programs to ensure staff is aware of protocols for protecting customer information.
- The Committee will conduct an annual risk assessment to ensure compliance with the FTC safeguards rule making recommendations as necessary.
- The Committee, working with responsible units and offices, shall monitor, evaluate, and adjust the Program considering the results of the risk assessment process.
- Areas that handle covered information will work with the Office of the General Counsel and Procurement Office, and other offices as appropriate, to make certain that service provider contracts contain appropriate terms to protect the security of covered data.

Risk Identification and Assessment

The Committee will work with all relevant areas of the University to identify potential and actual risks to security of information. Each School or Department head, or their designee, will conduct an annual security review, with guidance from the Committee. This process will consider risks to covered data and the safeguards currently in place to manage those risks including employee management and training; information systems, including network and software design, as well as information processing, storage, transmission, and disposal for both paper and electronic records; and security management, including the prevention, detection, and response to attacks, intrusions, or other system failures. Covered areas will be asked to identify a responsible individual to serve as that area's contact person with the Committee. It is the responsibility of the covered area to participate and ensure identified risks are appropriately addressed and mitigated.

Information Systems and Safeguards

While ITS bears primary responsibility for solutions, strategies, and administration of operational risk activities such as enterprise firewall management, vulnerability scanning, and annual penetration testing, all members of the university community are responsible for participation in managing and mitigating identified and potential risks.

ITS will assure the physical security of all ITS hosted systems which contain or have access to covered data and information. Systems under GLB which are not hosted by ITS must comply with GLB regulation and university information security policy. It is the responsibility of the covered area to ensure compliance of systems not hosted by ITS. The Committee will periodically review other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the University to risk. Destruction of devices and records will follow the university's secure destruction policies and standards and retention per regulatory or state retention requirements.

ITS provides a university-wide encryption solution for the transmission of sensitive data and provides encrypted storage and database specific solutions where feasible. Third party encryption solutions are required of vendors storing or transmitting sensitive information. It is the responsibility of each covered area to ensure that secure processes are utilized.

Covered areas will be responsible for maintaining and providing to ITS a list of GLB relevant devices and systems both managed and not managed by ITS. ITS will use this information to develop and maintain a registry of all GLB computers and systems. This registry will include device identification information, physical location, operating system, intended use (server, personal computer, lab machine, etc.), and the person, persons, or department primarily responsible for the machine.

While ITS provides enterprise solutions for system and software patching it is the responsibility of users/technical liaisons to ensure systems not managed by ITS which hold GLB data are properly registered with ITS and connected to the enterprise management infrastructure. ITS assumes the responsibility of assuring that patches for operating systems and/or software environments are made available in a timely manner and will keep records of patching activity. U of L will review its procedures for patches to operating systems and software and will keep current on potential threats to the network and its data.

PeopleSoft Campus Solutions (CS) is the primary system of use and storage of student information. ITS has designated a Director, Student Information Systems with primary responsibility for overseeing the technical operations of CS. While the University has discontinued use of social security numbers as student identifiers, it is however, still required for some purposes and therefore, student social security numbers remain in the University student information system. The University has taken steps to secure sensitive information within PeopleSoft (PS) limiting the amount of information that is displayed and encrypting all stored information. Security can be controlled down to the field level based on user profiles, roles and permission lists and access to PS pages and data is controlled. Access requests are handled by the CS Security Administrator and are reviewed for appropriateness and approved. Requests for changes to the CS system are handled via the ITS change management process which includes requestor validation, requirement identification, documentation, approval, and testing. Changes are tracked, reviewed, tested, and approved prior to moving to production. Changes that include a request for data imports/exports are reviewed by several areas which include the data owners and the Information Security Compliance and FERPA offices. External transmissions utilize encryption where sensitive data is involved and transmitting and receiving of data, once approved, follows a defined process.

Security and Incident Management

The University's Information Security Incident policy outlines responsibilities and procedures for reporting and addressing security incidents. ITS deploys tools such as next generation firewalls, intrusion detection and prevention systems (IDS/IPS), and a security information & event management (SIEM) to monitor and to detect any actual or attempted attacks on covered systems and follows procedures for addressing and remediating actual or attempted unauthorized access to covered data or information. The ITS SOC is responsible for monitoring and managing security alerts and events. ITS and the ISCO work in conjunction to identify, mitigate, and report incidents. The ISCO is responsible for managing breach response and notification of incidents. GLB applicability is part of the incident review process and the Department of Education is included in the notification protocol. GLB covered areas are responsible for development, communication, and training of specific response procedures; to work within the university defined Incident Response policies and procedures; and to follow reporting procedures in notifying ITS/ISCO.

ITS is responsible for disaster recovery services of university enterprise systems. It is the responsibility of each covered area to ensure appropriate Business Continuity Planning and DR requirements.

Employee Management and Training

As part of the University's employee onboarding process, employees are required to undergo a background check. Annual sanction checks are performed for employees and student workers. Relevant offices of the University may determine whether more extensive 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's Information Security Compliance Office (ISCO) provides university-wide information security awareness and training. Employees receive information regarding security policies and responsibilities at new employee orientation. Additionally, completion of an online security module and a compliance module is required of individuals within 30 days of employment. The ISCO and ITS provide ongoing security training via in person trainings, employee and student news publications, brochures, and digital communication channels. Additionally, targeted online training is also provided and required for those individuals with access to PI related to PCI, HIPAA and FERPA.

Specific FERPA/GLB training is provided via Blackboard and required prior to access to student systems and financials. As part of the Program, the Committee will ensure departments that handle covered information develop appropriate training programs to ensure staff is aware of protocols for protecting customer information. It is the responsibility of the covered area to ensure compliance with training requirements and information security practices. Non-compliance may result in sanctions in accordance with University and HR policy.

Oversight of Service Providers and Contracts

GLB requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. As part of the review process, vendors are required to disclose conflicts or disbarment and are included in the sanction check process. The Office of General Counsel has provided specific GLB compliance language informing vendors of their GLB compliance responsibilities for inclusion in Procurement's contract process. Additionally, in coordination with the ISCO, Procurement has implemented a process to review vendor security controls for external parties involved with sensitive information. It is the responsibility of each GLB covered area to maintain, update and periodically review a vendor inventory list and to work with the Office of the General Counsel, Procurement, and other offices as appropriate, to make certain that security reviews have been conducted and service provider contracts contain appropriate terms to protect the security of covered data.

V. GLB Information Security Program Evaluation and Reporting

GLB mandates that this Program be subject to periodic review, adjustment, and reporting. Processes in relevant offices of the University such as data access procedures and the training program should undergo regular review. The Program itself will be re-evaluated and updated annually by the Committee to assure ongoing compliance. As per the incident response process, incidents are reported to appropriate leadership and as required by regulation. Overall Program status will be reported annually.

VI. Policies, Programs and Guidelines

These policies, programs, and/or guidelines are established to facilitate compliance with information security programs

- Policy and Procedure Library (louisville.edu) - Information Security and Technology section
    - Backup of Data
    - Business Continuity and Disaster Recovery
    - Cloud Computing and 3rd Party Vendor Services
    - Data Facility Security
    - Electronic Data and Voice Mail Disclosure
    - Encryption of Data
    - Firewalls
    - HIPAA Privacy Policy
    - Information Security Responsibility
    - Internet Acceptable Use
    - Inventory, Tracking and Discarding of Computing Devices
    - Network Service
    - Passwords
    - Policy Exception Management Process
    - Protection from Malicious Software
    - Sanction Policy
    - Security Incidents

    - Server Computing Devices
    - Workstation and Computing Devices
- Pol-Employment Applications — Policy and Procedure Library (louisville.edu) – Criminal background checks
- Privacy Statement (louisville.edu) – University of Louisville Privacy Statement
- Personal Information Protection — Office of the Bursar (louisville.edu) – Personal Information Protection – Bursar – Non-Public Personal Information guidelines