Department Administrative Policy and Procedure

Subject: University of Wyoming Gramm-Leach-Bliley Act (GLBA) Safeguarding Customer Information
Number:

I. PURPOSE

The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA does not contain an exemption for colleges or universities; education entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, the University of Wyoming has adopted an Information Security Program (ISP) for certain highly critical and private financial and related information. This program applies to customer financial information (covered data) the University receives in the course of business as required by GLBA and other confidential financial information included within its scope.

A. Standards

The objectives of the ISP program are:

1. To ensure the security and confidentiality of customer information;
2. To protect against threats to the security or integrity of such information; and
3. To guard against unauthorized access to or use of such information.

II. DEFINITIONS

Covered data under the plan is defined by three categories:

Personal Identifiable Information (PII) – Also known as non-public personal information or protected data, PII includes social security numbers, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity.

Financial Information – Information that the University has obtained from faculty, staff, students, alumni, auxiliary services and patrons in the process of offering financial aid or conducting a program. Examples include direct deposit

banking information, making, servicing, and collecting loans, including payment plans, income, and credit histories.

Student Financial Information – Information that 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. Examples include student loans, income tax information received from a student's parent when offering a financial aid package (FAFSA), bank and credit card account numbers, and income and credit histories.

III. POLICY

A. Elements of the ISP

1. **Appointment of a qualified individual as coordinator:** The position of Chief Information Officer (CIO) is the individual designated by the University to coordinate the GLBA ISP.

2. **Written risk assessment:** At least annually, the GLBA ISP Coordinator shall provide a written report, identifying reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, along with the sufficiency of any safeguards in place to control these risks. The written report shall include the criteria used for evaluating the foreseeable risks and the existing safeguards.

3. **Implementation of safeguards to protect against risks identified in the risk assessment:** The GLBA ISP Coordinator shall work with heads of units to oversee their individual safeguarding programs. Specific safeguarding practices should include:
   - **a.** Conducting periodic written inventory of where covered data is collected, stored, and transmitted and designing safeguards to respond accordingly, including periodic review of access controls.
   - **b.** Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored. Ensuring windows are locked and using safes when practicable for especially sensitive data such as credit card information, checks, and currency.
   - **c.** Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as a result of their job.
   - **d.** Using and frequently changing passwords to access automated systems that process sensitive information, requiring multi-factor authentication for access to systems, and requiring identification before processing in-person transactions.
   - **e.** Using firewalls and encrypting information when feasible and using authentication and passwords when creating new accounts.

f. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information.

g. Shredding and erasing customer information when no longer needed in accordance with unit and University policy and the law.

h. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities.

i. Ensuring that agreements with third-party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance. Periodically reviewing changes in vendor applications to ensure continued safeguards are still in place.

j. Ensuring that software developed in-house or through third parties is developed using safeguarding provisions.

k. Maintaining user and activities logs through the Security Information and Event Management (SIEM) and watch for unauthorized access.

l. Discouraging the use of social security numbers and using social security numbers only in accordance with university policy on social security numbers.

4. **Testing:** The University will continually monitor systems for potential penetration and conduct penetration testing at least annually and publicly-known security vulnerabilities scans every six months or earlier if a material change to operations or systems occurs.

5. **Training**: The University shall ensure all new and existing employees who are involved in activities covered under this plan receive safeguarding and compliance training. A written agreement containing the employee's signature and attesting to the fact that he or she received training, is aware of University and Unit information policies and guidelines, and is aware of the importance the University places on safeguarding information, is required. Training should encompass the areas covered by this document.

6. **Vendor Selection:** The University will select service providers, that are given access to covered data in the normal course of business, that have the skills and experience to maintain appropriate safeguards. Agreements shall include security expectations and service providers' work shall be monitored and periodically assessed for suitability.

7. **ISP Maintenance:** The University will review and update, at a minimum, annually, the ISP through the Office of the Chief Information Officer (CIO), the Office of General Counsel, and the GLBA Working Committee, which is comprised of leaders representing Information Technology, Financial Services, Financial Aid, Admissions, and Risk Management.

8. **Written incident response plan:** The University's ISP incident response plan will be held in the office of the CIO.

9. **Reporting:** The GLBA ISP Coordinator shall report annually to the Board of Trustees to the Fiscal and Legal Affairs Committee the overall assessment of compliance, including risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how any events were managed and recommendations for changes to the ISP.

Responsible Division/Unit: Budget & Finance, Student Financial Services
Source: Gramm-Leach-Bliley Act (GLBA)
Links: http://www.uwyo.edu/regs-policies
Associated Regulations, Policies, and Forms: UW Regulation 8-1: Proper Use of Computing and Data Communication Facilities Operated by Division of Information Technology; Family Education Rights and Privacy Act (FERPA); Information Security Policy; Two-Factor Authenticiation.
Approved: 6/8/2023