INFORMATION SECURITY PROGRAM

Kansas Wesleyan University

Requirements

GLBA mandates the protection of consumer information's security, integrity, and confidentiality. To achieve GLBA compliance, organizations must establish, implement, and enforce a comprehensive information security program. This program should encompass administrative, technical, and physical safeguards that are deemed suitable for the institution and the data it handles. In addition to implementing their own safeguards, organizations are also responsible for ensuring that their affiliates and service providers effectively protect customer information entrusted to them. The United States Department of Education strongly encourages institutions of higher education to familiarize themselves with the standards outlined in NIST SP 800-171, the recognized information security publication for safeguarding "Controlled Unclassified Information" (CUI).

Risk Management and University Personnel

Kansas Wesleyan University personnel have the responsibility of identifying and evaluating risks, as well as managing and controlling them appropriately. Given the size and complexity of the University, a collaborative approach is employed for assessing and mitigating risks. This approach involves expertise in various areas, including but not limited to:

1. Vendor management and contracts
2. Human resource training
3. Systems, software, and network security
4. Legal considerations
5. Operational monitoring

By leveraging these areas of expertise, the University can effectively address potential risks and ensure the security and protection of sensitive information.

Actions Required and Taken

Kansas Wesleyan University has fulfilled the necessary requirements to ensure compliance with the Gramm-Leach-Bliley Act (GLBA). The university's efforts in this regard are an ongoing process, continuously evolving and subject to regular review to uphold the utmost standards of data security. The following items listed below were taken.

1. Implement and periodically review access controls:
    - Develop and enforce access control policies and procedures.
    - Regularly review and update user access privileges based on job roles and responsibilities.
    - Conduct periodic access control audits to identify and mitigate any vulnerabilities or unauthorized access.
2. Conduct a periodic inventory of data:
    - Perform regular data inventory assessments to identify the collection, storage, and transmission points of customer information.
    - Maintain an up-to-date record of data inventory, including its location, sensitivity level, and associated systems or applications.
3. Encrypt customer information:
    - Implement encryption mechanisms for customer information stored on the institution's systems.
    - Utilize secure and encrypted transmission protocols when transferring customer information.
    - Establish encryption policies and procedures that comply with industry standards.
4. Assess institution-developed apps:
    - Conduct thorough security assessments of institution-developed applications.
    - Identify potential vulnerabilities and implement necessary security measures to mitigate risks.
    - Regularly update and patch applications to address security flaws.
5. Implement multi-factor authentication:
    - Require multi-factor authentication for anyone accessing customer information on the institution's systems.
    - Utilize a combination of factors such as passwords, biometrics, tokens, or smart cards to verify user identity.
    - Enforce strong password policies and educate users about the importance of safeguarding their credentials.
6. Secure disposal of customer information:
    - Establish procedures for the secure disposal of customer information.
    - Ensure proper data destruction methods, such as shredding physical documents or using secure data erasure techniques for electronic media.
    - Document disposal activities to demonstrate compliance with disposal policies.
7. Anticipate and evaluate changes to the information system or network:
    - Regularly assess and evaluate the institution's information systems and network for potential vulnerabilities or changes that may impact security.
    - Conduct risk assessments to identify emerging threats and implement appropriate safeguards.
    - Stay updated with security industry best practices and regulatory requirements.

8. Maintain activity logs and monitor unauthorized access:
    - Maintain comprehensive logs of authorized users' activity, including access attempts and actions performed.
    - Implement log monitoring and analysis mechanisms to detect and investigate suspicious activities or unauthorized access.
    - Establish incident response procedures to address security incidents promptly.

- ## Coordination and Responsibility for the Information Security Program

The Information Security Program's Coordinator is the AVP of I.S. for Kansas Wesleyan University. The coordinator has also been designated as the Chief Information Security Officer. The coordinator is responsible for the development, implementation, and oversight of Kansas Wesleyan University's compliance with the policies and procedures required by the Gramm Leach Bliley Act's Safeguards Rule.

Although ultimate responsibility for compliance lies with the Coordinator, representatives from each operational area developing, implementing, and overseeing are responsible for implementing and maintaining the specified requirements of the security program in their specific operation.

- ## Safeguards and Risk Assessment

Protecting personal information involves acknowledging the potential risks associated with its handling and storage. By identifying areas of vulnerability and implementing suitable safeguards, the overall risk can be significantly reduced. These safeguards encompass protective measures for both information systems and physical storage of paper documents.

1. The University has implemented a variety of safeguards to protect the confidentiality, integrity, and availability of the University's information systems and the data they contain. These safeguards include:
2. Access control: Access to systems and data is restricted to authorized users. Access is granted based on the user's role and need to know.
3. Data encryption: Data is encrypted both in transit and at rest.
4. Data backup: Data is backed up regularly to ensure that it is available in the event of a system failure or other disaster.
5. Firewalls: Firewalls are used to protect the University's systems and data from unauthorized access.
6. Network monitoring: Network traffic is monitored passively.

- ## Employee Training and Education

Departments must also ensure that all employees are aware of the applicable policies and procedures related to protected information. These policies and procedures should be reviewed and updated regularly to ensure that they are up to date and reflect the current state of the organization. Additionally, departments should be aware of any changes to applicable laws and regulations that could affect the handling of protected information. Finally, departments should ensure that all employees are aware of the consequences of mishandling protected information. Employees should understand that there may be disciplinary action taken if they fail to adhere to the policies and procedures related to protected information.

- ### Oversight of Service Providers and Contracts

The University will also require service providers to comply with applicable laws and regulations, including the GLBA. The University will conduct periodic reviews of service providers to ensure they are meeting the requirements of the Act. The University will also require service providers to submit written assurances that they are in compliance with the GLBA.

- ### Evaluation and Revision of the Information Security Program

The Information Security Program is also reviewed on an annual basis by the AVP of I.S. This review includes an assessment of the effectiveness of the program, an evaluation of the current risks, and a review of any changes in the laws and regulations that may affect the program. The review also includes information concerning data access procedures and training programs. The results of the review are documented, and any necessary changes will be implemented.

VI. Definitions

1. According to the FTC Safeguard Rules §314.2.c, an Information Security program refers to the measures taken to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information, including administrative, technical, and physical safeguards.
2. In accordance with the GLBA, a 'consumer' is defined as an individual who obtains financial products or services from a financial institution primarily for personal, family, or household purposes. This term also includes the legal representative of such an individual (refer to 15 U.S.C. § 6809(9)).
3. Under the GLBA, a 'customer' is a consumer who maintains an ongoing relationship with a financial institution. A 'customer relationship' denotes a continuous association with a consumer.

4. Non-public personal Information: The GLBA safeguards the privacy of non-public personal information, which encompasses various types of sensitive data such as personal addresses, phone numbers, health information, financial information, driver's license numbers, bank account information, credit card numbers, credit reports, loan applications, loan details, social security numbers, tax returns, and more.
5. Customer Information: According to the GLBA FTC Safeguard Rules §314.2.b, customer information refers to any record, in paper, electronic, or other form, that contains non-public personal information as defined in 16 CFR 313.3(n) about a customer of a financial institution. Such records are handled or maintained by you or your affiliates.
6. Personal Data: Personal data pertains to any information concerning an identified or identifiable natural person (data subject). An identifiable natural person is someone who can be directly or indirectly identified, typically through a name, identification number, location data, online identifier, or other specific factors related to their physical, physiological, genetic, mental, economic, cultural, or social identity.
7. Processing: The term 'processing' encompasses any operation or series of operations performed on personal data, whether automated or not. These operations include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or any other form of making the data available, alignment or combination, restriction, erasure, or destruction.
8. Data protection by design is an approach that prioritizes privacy and data protection considerations during the design phase of systems, services, products, or processes. It also ensures ongoing attention to these issues throughout their lifecycle.
9. Data protection by default requires that you only process the data necessary to achieve your specific purpose. This principle aligns with the fundamental data protection principles of data minimization and purpose limitation.
10. Third Party: In the context of data protection, a third party refers to a natural or legal person, public authority, agency, or body that is not the data subject, controller, processor, or anyone under the direct authority of the controller or processor who is authorized to process personal data.
11. Personally Identifiable Information (PII): PII encompasses any information that relates to an identified or identifiable living individual. It includes various data elements that, when collected together, can lead to the identification of a specific person.

Legal References

- Gramm-Leach-Bliley Act: The legal provisions related to the Gramm-Leach-Bliley Act can be found in Title 15 of the United States Code, specifically in Subchapter I, sections 6801 to 6809.

- Health Insurance Portability and Accountability Act of 1996: The relevant legislation is Public Law Number 104-191, which can be found in Volume 110 of the United States Statutes at Large, page 1936. This law has been codified in various sections of Title 18, Title 26, Title 29, and Title 42 of the United States Code.
- Privacy Regulations: The regulations pertaining to privacy are outlined in Title 16 of the Code of Federal Regulations, specifically in Part 313. For reference to the Family Educational Rights and Privacy Act (FERPA), please consult this section.
- Family Educational Rights and Privacy Act (FERPA): The FERPA provisions can be found in Title 20 of the United States Code, Chapter 31, specifically in section 1232g.
- FERPA regulations: The regulations related to FERPA can be found in Part 99 of Title 34 of the Code of Federal Regulations.
- Safeguard Regulations: The regulations pertaining to safeguards can be found in Part 314 of Title 16 of the Code of Federal Regulations. These regulations were published in the Federal Register on May 23, 2002.
- HIPAA Security Regulations: The relevant regulations can be found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations. Additionally, reference can be made to the Federal Register, Volume 68, page 8334, published on February 20, 2003.
- NACUBO Advisory Report 2003-01: This advisory report was issued on January 13, 2003, by the National Association of College and University Business Officers (NACUBO).
- FTC Facts for Business: Financial Institutions and Customer Data: Complying with the Safeguards Rule: This publication was released in September 2002 by the Federal Trade Commission (FTC) and provides information on how financial institutions can comply with the Safeguards Rule.