Privacy of Personal Information

CHSU is committed to protecting the security and confidentiality of students' personal information consistent with the requirements of federal and state laws and regulations. This includes protection of students' financial aid information from threats and hazards to its security and the protection of private information against unauthorized access to the information.

The Gramm-Leach-Bliley Act, (GLBA) requires the development of an Information Security Program for the protection and safeguarding of customer non-public personal information (PII) associated with financial services held by financial institutions. For purposes of the Safeguards Rule, customer information includes information obtained by providing financial services (including administering Title IV student loan programs and institutional loans and certifying private education loans) to current or former students.

Key compliance requirements include:

- Designating an employee to coordinate an information security program.
- Identifying risks to the security of customer information and computer information systems.
- Providing employee training and management in a security awareness program.
- Documenting and maintaining safeguards for risks identified.

CHSU is responsible for taking reasonable and appropriate steps to protect the confidentiality, availability, privacy, and integrity of information in its custody. This includes protecting the security and integrity of the equipment where private information is processed and maintained, and preserving information in case of intentional, accidental, or natural disaster. In addition, CHSU is responsible for the maintenance and currency of applications that use this information.

CHSU Information Security Policies are applicable to all data, systems and equipment that contain protected, confidential or mission critical data, including college and departmental level system and equipment, and vendor hosted solutions. The policies are applicable regardless of whether the information or equipment is on- or off-campus and whether maintained by CHSU's Information Technology staff or by an external vendor or consultant.

To comply with GLBA and the Safeguards Rule, CHSU has implemented the following steps:

- Designated the President as the ultimately responsible party for the University's information security program, with authority for implementing and enforcing the security program delegated to the Executive Director of IT and the Assistant Director of Financial Aid.
- Not collecting personally identifiable information unless the University's need for the information has been clearly established.
    - Personally identifiable information collected will be adequately protected from unauthorized disclosure.
    - Personally identifiable information collected will only be stored when relevant to the purpose for which it has been collected.
- Utilizing the outcome of the risk assessment and evaluation process to design and implement additional safeguards through the following:
    - Implementing technical and physical access controls that will authenticate users and limit users' access to the information, they need to perform their duties.
    - Limiting access to personally identifiable information to: (a) authorized CHSU employees with a valid related business need to access, modify, or disclose that information; (b) to the individuals about whom the data applies; and (c) appropriate legal authorities.
    - Requiring that University Colleges and Departments administer plans and procedures for protection of their data. The plans must include access control, password security, backup and off-site storage of mission critical data, security systems that provide protection against known vulnerabilities.
    - Evaluating and adjusting the University's information security program based on: (a) the risk assessments, testing and monitoring procedures outlined in these rules; (b) material changes to CHSU's operations or business arrangements; and (c) any other circumstances that may have a material impact on the information security program.

    - Developing, implementing, and maintaining procedures for the secure disposal of information in any format no later than two years after your most recent use of it to serve the customer. unless the information is required for business operations, other legitimate business purposes, law or regulation requires retention, or targeted disposal is not reasonable.
- Conducting periodic risk assessments and evaluations of the adequacy of existing safeguards in protecting against reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of private information
- Developing a written information security program that includes the implementation of the minimum safeguards listed on Appendix A.
- Implementing a program of regular audits and testing to assess and monitor the effectiveness of the safeguards.
- Implementing an information security awareness and training program for all employees with access to protected data and providing staff with strategic procedures on how to protect data.
- Addressing how the University oversees information system service providers in selecting qualified service providers, requiring that service provider implement and maintain safeguards similar to those utilized by the University, and regularly evaluating service providers for consideration in risk management processes.

In compliance with the Family Educational Rights and Privacy Act (FERPA) and the GLBA, students who do not want to have any information disclosed have the option to "opt-out" of information being disclosed. The request form to "opt-out" of information disclosure must be submitted to the Office of the Registrar. *(The complete policy on CHSU Privacy of Personal Information is located on the CHSU website at https://chsu.edu/policies)*

APPENDIX A:

FTC SAFEGUARDS RULE: MINIMUM SAFEGUARDS FOR WRITTEN INFORMATION SECURITY PROGRAM

1. Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:
    - Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and
    - Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;
2. Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;
3. Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;
4. Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
5. Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;
6. Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and periodically review your data retention policy to minimize the unnecessary retention of data;
7. Adopt procedures for change management; and
8. Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.