REG 08.00.06
GLBA Required Information Security Program

Authority: Vice Chancellor for Finance and Administration

History:

- Effective Date: May 23, 2003
- Revised August 21, 2018

Related Law:

- Gramm-Leach-Bliley Act
- Federal Student Aid GLBA Information

Contact Information: Associate Vice Chancellor of Information Resources and CIO, (910) 775-4888

1. PURPOSE

1.1 This document summarizes the comprehensive written information security program (the "Regulation") of the University of North Carolina at Pembroke (UNCP), as mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this Regulation describes the program elements pursuant to which UNCP intends to:

1.1.1 Ensure the security and confidentiality of covered records

1.1.2 Protect against any anticipated threats or hazards to the security of such records

1.1.3 Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to faculty, staff or students.

1.2 The Regulation incorporates by reference the institution's policies and procedures, enumerated below, and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

2. DESIGNATION OF REPRESENTATIVES

2.1 The Associate Vice Chancellor for Information Resources and Chief Information Officer (CIO) is designated as the Program Officer who shall be responsible for coordinating and overseeing the Regulation. The Program Officer may designate other representatives of the institution to oversee and coordinate particular elements of the Regulation. Any questions

regarding the implementation of the Regulation or the interpretation of this document should be directed to the Program Officer or his/her designees.

3. SCOPE

3.1 The Regulation applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the institution or its affiliates.

3.2 For these purposes, the term nonpublic financial information shall mean any information

3.2.1 A student or other third party provides in order to obtain a financial service from the institution,

3.2.2 About a student or other third party resulting from any transaction with the institution involving a financial service, or

3.2.3 Otherwise obtained about a student or other third party in connection with providing a financial service to that person.

4. ELEMENTS OF THE REGULATION

4.1 Risk identification and assessment UNCP has tools and processes in place to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Regulation, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the institution's operations, including:

4.1.1 Employee training and management: The Program Officer will coordinate with representatives in the institution's Financial Aid office to evaluate the effectiveness of the institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the institution's current policies and procedures in this area, including the Student Handbook (specifically, "Policies Concerning Student Records"), the Faculty Handbook, the Staff Handbook and the policies and procedures of the Office of Business Affairs.

4.1.2 Information Systems and Information Processing and Disposal: The Program Officer will coordinate with representatives of the institution's Division of Information Technology (DoIT) to assess the risks to nonpublic financial information associated with the institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. The Program Officer will assess the institution's current policies and procedures relating to acceptable use of the institution's network and network security, document retention and destruction. The Program Officer will also coordinate with the institution's DoIT to assess procedures for monitoring potential

information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

4.1.3 Detecting, Preventing and Responding to Attacks: The Program Officer will coordinate with the DoIT staff and other relevant units to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the DoIT the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the institution.

4.2 Designing and Implementing Safeguards: The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

4.3 Overseeing Service Providers: The Program Officer shall coordinate with those responsible for the third-party service procurement activities among the DoIT and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officer will work with the Office of General Counsel or other designated institutional official to develop and incorporate standard, contractual protections applicable to third-party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Office of General Counsel or other designated institutional official. These standards shall apply to all existing and future contracts entered into with such third-party service providers.

4.4 Adjustments to Program: The Program Officer is responsible for evaluating and adjusting the Regulation based on the risk identification and assessment activities undertaken pursuant to the Regulation, as well as any material changes to the institution’s operations or other circumstances that may have a material impact on the Regulation.

5. RESPONDING TO SECURITY AND ABUSE INCIDENTS:

5.1 All users have the responsibility to report any discovered unauthorized access attempts or other improper usage of UNCP computers, networks, or other information processing systems. If a security or abuse problem with any university computer or network facility is observed by or reported to a user, such user shall immediately report the same to the DoIT.

6. RANGE OF DISCIPLINARY SANCTIONS

6.1 Persons in violation of this Regulation are subject to a full range of sanctions, including, but not limited to, the loss of computer or network access privileges, disciplinary action, and dismissal from UNCP. Any sanctions against employees will be imposed through procedures consistent with any applicable state regulations. Some violations may constitute criminal or civil offenses, as defined by local, state, and federal laws and the university may prosecute any such violations to the full extent of the law.

6.2 UNCP may suspend computer or network access privileges immediately and without prior notice to the user if necessary to preserve the safety or integrity of UNCP's network or to prevent or investigate violation of applicable federal, state or local law or UNCP policy.