UNIVERSITY SYSTEM OF NEW HAMPSHIRE

Gramm-Leach-Bliley Act Information Security Program

PROGRAM:

Gramm-Leach-Bliley Act (GLBA) Information Security Program

STATEMENT:

This document summarizes the University System of New Hampshire's comprehensive written information security program in accordance with the Federal Trade Commission's Safeguards Rule, codified at 16 CFR Part 314, and the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801.

BACKGROUND:

The Gramm-Leach-Bliley Act (GLBA) is a Federal law which requires "financial institutions" to ensure the security and confidentiality of customers' personal information. To the extent colleges and universities offer "financial products or services" - primarily student loan activities – they are considered financial institutions under the GLBA. The University System of New Hampshire and its component institutions must take active steps to comply with the Safeguards Rule of the GLBA. The Safeguards Rule requires financial institutions, including colleges and universities, to develop an information security program to protect customer information.

APPLICABILITY:

The GLBA Information Security Program applies to any "customer information" that is handled or maintained by the University System of New Hampshire or its component institutions. Customer information includes nonpublic financial information (i) that a student or other third party provides in order to obtain a financial service from the University System of New Hampshire; (ii) about a student or other third party resulting from any transaction with the University System of New Hampshire involving a financial service; or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. "Customer information" and "financial service" are defined below. In general, this Program is applicable to financial transactions such as loans in which credit is extended and/or credit history information is obtained by USNH. Financial Aid and other services offered by USNH institutions may fall within the scope of this Program.

DEFINITIONS:

Customer Information is defined by federal law as any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the institution

or its affiliates. "Nonpublic personal information" includes personally identifiable financial information that is not publically available. Examples include customers' names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers that are provided by a customer to obtain a financial product or service. "Customers" of the University System of New Hampshire and its component institutions may include students, employees, alumni and other third parties.

Financial Service is defined by federal law to include, but is not limited to, such activities as the lending of money; investing for others; providing or underwriting insurance; giving financial, investment or economic advisory services; marketing securities and the like. Services involving the extension of credit are covered by this Program, but installment contracts (where no interest is charged) are not included.

Service Provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to an institution for the provision of a Financial Service. Examples include third-party collection agencies and systems support providers.

GUIDING PRINCIPLES/PURPOSE:

This document describes the elements of the GLBA Information Security Program pursuant to which the University System of New Hampshire intends to (i) ensure the security and confidentiality of Customer Information, (ii) protect against any anticipated threats or hazards to the security of such information, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to any customer.

RESPONSIBILITIES:

The University System of New Hampshire Information Security Committee (ISC) is responsible for coordinating and overseeing the information security program. The ISC may designate other representatives of the University System of New Hampshire or its component institutions to oversee and coordinate particular elements of the GLBA Information Security Program, including specific controls for ensuring security of Customer Information at the campus level, particularly with respect to the provision of student financial aid and student loans. Any questions regarding implementation or the interpretation of this document should be directed to the ISC.

ADMINISTRATION AND IMPLEMENTATION:

1. *USNH Information Security Committee (ISC)*: The University System of New Hampshire Information Security Committee (ISC) exists and operates under the authority of the USNH Information Technology Executive Committee (ITEC). The ISC includes representation from each USNH institution and the USNH

System Office. The ISC collaborates with institutional personnel to reduce information security risk for both shared and local information services and systems.

2. *Risk Identification and Assessment.* The ISC will lead the effort to identify and assess external and internal risks to the security, confidentiality, and integrity of Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. Working with campus subject matter business experts, the ISC will establish procedures for identifying and assessing such risks in each relevant area of the University System of New Hampshire's operations and those of its component institutions. University System of New Hampshire Internal Audit will incorporate GLBA risks into its annual audit plan.
3. *Employee training and management.* The ISC will coordinate with representatives in University System of New Hampshire's offices to ensure effectiveness of the University System's procedures and practices relating to access to and use of student records, including financial aid information, in the provision of Financial Services.
4. *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 ISC or its designee(s), will, on a regular basis, implement or recommend safeguards to control the risks identified. The ISC and/or its designee(s) will regularly test or otherwise monitor the effectiveness of such safeguards. The safeguards program will include, but not be limited to:
    - Information security access guidelines for the following areas, in accordance with policy USY VI.F.5.7:
        - Physical security of electronic and paper records;
        - Electronic commerce;
        - Disposal of records;
        - Detection and prevention of attacks, and other system failures (testing and monitoring); and
        - A process for periodic assessment and adjustment, and management of any material changes to business operations including a mechanism to adapt safeguards to new and emerging trends.
5. *Overseeing Service Providers.* The ISC or its designee(s) shall coordinate with those responsible for contracting with third-party Service Providers within the University System of New Hampshire and its component institutions to raise awareness of, and to institute methods for, selecting and retaining only those Service Providers that are capable of maintaining appropriate safeguards for Customer Information to which they will have access. In addition, the ISC will work with the Office of General Counsel and procurement offices to develop and incorporate standard, contractual protections applicable to third-party Service

Providers, which will require such providers to implement and maintain appropriate safeguards.

6. *Adjustments.* The ISC is responsible for evaluating and adjusting the GLBA Information Security Program based on the risk identification and assessment activities undertaken, as well as any material changes to the University System's operations or other circumstances that may have a material impact.

APPROVAL:

Approved by the University System of New Hampshire's Administrative Board on September 21, 2017.

REVIEW CYCLE:

This program will be reviewed and updated as needed, at least annually.