



Information Security and Privacy Gramm-Leach-Bliley Policy

Original Date: May 22, 2003

Revised Date: September 5, 2018

1.0 Overview and Purpose

The Gramm-Leach-Bliley Act (GLB) was enacted in 1999 and affects all financial institutions. Colleges and universities fall under GLB as part of financial lending and alumni processes. The GLB Financial Privacy Rule requires financial institutions provide a privacy notice at the time the consumer relationship is established and annually thereafter. It defines the protection of non-public personal information (NPI). It also requires institutions to implement thorough administrative, technical and physical safeguards to protect against any anticipated threats or hazards to the security or integrity of such information.

The College's written information security plan addresses the administrative, technical and physical safeguards mandated by the Federal Trade Commission's Safeguards Rule of the Gramm-Leach-Bliley Act (GLB). The College's information security policies ensure the security and confidentiality of customer information, protect against any anticipated threats to the security or integrity of such information, and guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

This document outlines NECO's general policy on GLB.

2.0 Applicability

GLB applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the college, whether in paper, electronic or other form, which is handled or maintained by, or on behalf of NECO or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from NECO, (ii) about a student or other third party resulting from any transaction with NECO 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.

3.0 Definitions

Financial Service: A "financial service" is defined by federal law to include, but not be 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.



Customer Information: Any record containing nonpublic personal information¹ about a customer of a financial institution, whether in paper, electronic, or another form, that is handled or maintained by or on behalf of the College and its affiliates.

Information Security Program: means the administrative, technical, or physical safeguards the College uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

4.0 Administration and Implementation

1. *Responsibilities.* The Director of Enterprise Technology is responsible for coordinating and overseeing NECO's Information Privacy and Security Policies and Practices.
2. *Risk Identification and Assessment.* NECO's Information Privacy Committee will identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information. This identification and assessment includes audits and employee training and management.
3. *Designing and Implementing Safeguards.* The Information Privacy Committee will work with departments to implement safeguards to control the risks identified through the audits.
4. *Overseeing Service Providers.* All Services Providers that store, transmit or receive nonpublic personal information must incorporate specific language into NECO contracts stating that the Service Provider will protect the NECO's nonpublic personal information according to commercially acceptable standards and no less rigorously than it protects its own information.
5. *Adjustments.* The Director of Enterprise Technology is responsible for evaluating and adjusting information privacy and security practices and policies based on the risk identification and assessment activities undertaken, as well as any material changes to NECO's operations or other circumstances that may have a material impact it.

5.0 Enforcement

Employees at NECO are required to abide by an institutional confidentiality agreement that states "I understand and agree that I will maintain in confidence and take steps to secure and protect all information that comes to me in the course of my relationship with NECO. I will not share this information with others who do not have a business need to know the information. When there is a business need that exists to share this information, I will do so in a manner that limits the possibility of the information being disseminated beyond those persons with a need to know. I agree to abide by the policies and practices expressed in this document."

6.0 Policy Support Contact

- **Gramm-Leach-Bliley (GLB) Compliance Representatives**
Federal Trade Commission Rule
16 C.F.R. § 314
Gramm-Leach-Bliley Act 2000

¹ 16 CFR Part 313.3(n)(1) defines nonpublic personal information as "personally identifiable information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." An example for colleges and universities would be information that a student provides on the FAFSA.



New England College of Optometry

- **NECO Financial Privacy Representatives**

Business Office:

Pete Maddocks , Controller
Business Office
424 Beacon Street, Boston MA 02115
617-587-5633

Information Technology:

Jill Lund, Director of Enterprise Technology
424 Beacon Street, Boston, MA 02115
617-587-5641

Financial Aid Office:

Esther Bamboo-Gomes, Director of Financial Aid
424 Beacon Street, Boston, MA 02115
617-587-5651

Human Resources:

Elizabeth Davies, Director of Human Resources
424 Beacon Street, Boston, MA 02115
617-266-2030