Gramm-Leach-Bliley (GLB) Policy

1.0 Overview

The Gramm-Leach-Bliley Act (GLB) was signed into law in 1999 and affects any institution that provides a “financial service.” Colleges and Universities fall under GLB as part of student lending and alumni processes. GLB requires colleges and universities to provide a privacy notice to students and restrict the non-public personal information (NPI) they share about students with third parties. It also requires institutions to implement thorough administrative, technical and physical safeguards.

WPI’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). This document outlines WPI’s general policy on GLB.

2.0 Definition

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.

3.0 Policy

APPLICABILITY:

GLB applies to any record containing nonpublic financial information about a student or other third party who has a relationship with WPI, whether in paper, electronic or other form, which is handled or maintained by, or on behalf of WPI 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 WPI;

(ii) about a student or other third party resulting from any transaction with WPI 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.

ADMINISTRATION AND IMPLEMENTATION:

1. *Responsibilities*. WPI's Chief Information Security Officer is responsible for coordinating and overseeing WPI's Information Security Program; GLB is a component of that program.
2. *Risk Identification and Assessment.* As part of WPI's Written Information Security Plan, we will identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information. This identification and assessment includes:

    - *Assessments*. On a routine basis, WPI will perform data privacy assessments for areas affected by GLB to assess risks. The Chief Information Security Officer will work with departments on any items that need remediation.
    - *Employee training and management.* In addition to the general information security training that all staff members are required to review on a yearly basis, staff in WPI's Financial Aid, Bursar's Office, and Advancement offices will also be required to review WPI's GLB Policy, FERPA Policy and any departmental procedures on GLB. This review should be done on a yearly basis as part of WPI's on-going training efforts.
    - *Information Systems and Detecting, Preventing and Responding to Attacks.* WPI will identify reasonably foreseeable risks to Information Systems and address detection, prevention and responding to attacks through the procedures outlined in WPI's Written Information Security Plan.

3. *Designing and Implementing Safeguards.* The Chief Information Security Officer will work with departments to implement safeguards to control the risks identified through the assessments mentioned above.
4. *Overseeing Service Providers.* As part of WPI's Third Party Assurance process, and under the direction of General Counsel, all services providers that store, transmit or receive Restricted Use data must incorporate language into WPI contracts stating that the service provider will protect WPI's Confidential Information according to commercially acceptable standards and no less rigorously than it protects its own confidential information. For vendors that provide Software As-A-Service (SaaS) solutions, WPI also requires vendors complete a Third Party Assurance requirements reviewed by the General Counsel, CIO, and the Chief Information Security Officer.

Adjustments. The Chief Information Security Officer is responsible for evaluating and adjusting the GLB Policy based on the risk identification and assessment activities undertaken, as well as any material changes to WPI's operations or other circumstances that may have a material impact it.

4.0 WPI Contact Roles

CONTACT PERSON
John Schwartz – Chief Information Security Officer (CISO)
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-6868

5.0 Enforcement

Any person that violates any of the measures found in this policy will be subject to the same disciplinary actions outlined in WPI's Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

6.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 11/06/2018.

Policy Reviewed Annually By: John Schwartz (CISO)

Related University Policies:

Written Information Security Plan (WISP)

Last Modified: 10/30/19