Last Reviewed: November 2023

Bentley University GLBA Policy

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 to 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 university'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 the university'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 university, whether in paper, electronic or other form, which is handled or maintained by, or on behalf of Bentley University 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 Bentley University, (ii) about

a student or other third party resulting from any transaction with Bentley University 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.

4.0 Administration and Implementation

1. *Responsibilities*. The Chief Information Security Officer is responsible for coordinating and overseeing the university's Written Information Security Program.
2. *Risk Identification and Assessment.* As part of the university'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:
    - *Audits*. On a routine basis, the university will perform audits for areas affected by the GLB Act to assess risk. The Information Security and Privacy Administrator 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 an annual basis, staff in the university's specific offices will also be required to review the university's GLB Policy, FERPA Policy and any departmental procedures on GLB. This review should be done on an annual basis as part of the university's on-going training efforts.
    - *Information Systems and Detecting, Preventing and Responding to Attacks.* The university will identity reasonably foreseeable risks to Information Systems and address detection, prevention and responding to attacks through the procedures outlined in the university's written information security plan.
3. *Designing and Implementing Safeguards.* The CISO will work with departments to implement safeguards to control the risks identified through the audits mentioned above.
4. *Overseeing Service Providers.* As part of the university's Third Party Assurance process, and under the direction of General Counsel, all Services Providers that store, transmit or receive nonpublic personal information must incorporate specific language into university contracts stating that the Service Provider will protect the university's nonpublic personal information according to commercially acceptable standards and no less rigorously than it protects its own information. A Third Party Assurance Questionnaire must be completed and reviewed by the General Counsel, and the CISO.
5. *Adjustments.* The Information Security and Privacy Administrator is responsible for evaluating and adjusting the GLB Act Policy based on the risk identification and assessment activities undertaken, as well as any material changes to the university's operations or other circumstances that may have a material impact it.

5.0 Exceptions

Any exceptions to this policy are to be reviewed and approved by the CISO in consultation with General Counsel.

6.0 Enforcement

As described in Bentley's Acceptable Use Policy, anyone found to have violated this policy may be subject to disciplinary action, up to and including immediate termination.

7.0 Policy Support Contact

- Chief Information Security Officer
- cybersecurity@bentley.edu

8.0 Supporting Documentation

This policy is supported by the following policies, procedures, and/or guidelines.

- Acceptable Use Policy

Revision History

Version	Date	Author	Reviewers	Approvers	Notes
1.0	7/13/2010			Data Privacy Committee	
2.0	09/30/2013			Data Privacy Committee	
2.1	11/10/2023	David Norman CISO			Minor edits and updates to the policy to reflect changes in personnel and procedures