Becker's Gramm-Leach-Bliley (GLB) Policy

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.

Becker'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 Becker's general policy on GLB.

APPLICABILITY:

GLB applies to any record containing nonpublic financial information about a student or other third party who has a relationship with Becker College, whether in paper, electronic or other form, which is handled or maintained by, or on behalf of Becker College 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 Becker College, (ii) about a student or other third party resulting from any transaction with Becker College 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.

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.

ADMINISTRATION AND IMPLEMENTATION:

1. *Responsibilities*. Becker Chief Financial Officer and Chief Information Officer are responsible for coordinating and overseeing Becker's Information Security Program; GLB is a component of that program.
2. *Risk Identification and Assessment.* As part of Becker'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, Becker will perform audits for areas affected by GLB to assess risks. The Chief Information 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 Becker's Financial Aid, Financial Operations, and College Advancement offices will also be required to review Becker's GLB Policy, FERPA Policy and any departmental procedures on GLB. This review should be done on a yearly basis as part of Becker's on-going training efforts.
- *Information Systems and Detecting, Preventing and Responding to Attacks.* Becker will identity reasonably foreseeable risks to Information Systems and address detection, prevention and responding to attacks through the procedures outlined in Becker's Written Information Security Plan.

3. *Designing and Implementing Safeguards.* The Chief Information Officer will work with departments to implement safeguards to control the risks identified through the audits mentioned above.
4. *Overseeing Service Providers.* As part of Becker's Third Party Assurance process, and under the direction of the Chief Financial Officer, all Services Providers that store, transmit or receive confidential information must incorporate language into Becker contracts stating that the Service Provider will protect Becker'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 solutions for Becker (hosted solutions), Becker also requires vendors to complete a Third Party Assurance Questionnaire reviewed by the General Counsel, COO, Director of Enterprise Infrastructure and the Chief Information Security Administrator.
5. *Adjustments.* The Chief Financial Officer and Chief Information Officer are responsible for evaluating and adjusting the GLB Policy based on the risk identification and assessment activities undertaken, as well as any material changes to Becker College's operations or other circumstances that may have a material impact it.

ENFORCEMENT:

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

APPROVAL:

Approved by Becker's Information Security Advisory Committee on February 23, 2012.

REVIEW CYCLE:

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