The Gramm-Leach-Bliley Act

The Gramm Leach Bliley Act (GLBA) is a law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information (Educause, GLB Act).

GLBA requirements

GLBA regulations include both a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both of which are enforced by the Federal Trade Commission (FTC) for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA).

Privacy Rule

The GLBA Financial Privacy Rule was created to regulate the collection and disclosure of nonpublic personal information between a financial institution and its customers.

Safeguards Rule

The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care (Electronic Code of Federal Regulation, Part 314).

Under this mandate, Belhaven University is required to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue. Such safeguards shall include measures that:

1. Ensure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Compliance with GLBA

- The University has designated an official Program Officer, based in the office of Information Technology, who enforces security polices approved by the Administrative Team.
- University units that are significantly engaged in financial activities that involve the collection or utilization of customer financial information must identity themselves to the University's Customer Information Security Officer. Examples of activities that GLBA would apply to include administering financial aid, processing of credit card information, and collecting of any other form of customer financial information. University units must document all such collection and processing activities. They must describe the nature and extent of their utilization of customer information. And an employee must be appointed to oversee the unit's information safeguards practices.
- University units must assess their current customer information practices, identify vulnerabilities, and take appropriate measures to secure customer information.