GLBA

Gramm-Leach-Bliley Act (GLBA), commonly pronounced “glibba”.

General Information

GLBA was enacted by Congress in 1999 to reform the banking industry. Colleges and universities are also subject to some of the provisions of GLBA because of the collection and maintenance of financial information of students and interactions with others. This requirement falls under the institution’s Program Participation Agreement (PPA) with the U.S. Department of Education. Within the last two years there has been a heightened alert to protection of personal information. Higher education has become a prime target of hackers due to the vulnerability of students.

July 29, 2015 – Dear Colleague letter was sent by ED alerting schools of the GLBA requirements.

July 1, 2016 – Dear Colleague letter was sent by Ed alerting schools of the GLBA requirements.

November 27, 2017 – The Government Accountability Office (GAO) issued a report stating an audit of ED’s FSA procedures found several weaknesses in procedures for protecting student records.

February, 2018 – The most recent audit guide will be released with newly added questions regarding cybersecurity.

Requirements – U.S. Department of Education

- Develop, implement, and maintain a written information security program;
- Designate the employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement an information safeguards program;
- Select appropriate service providers that are capable of maintaining appropriate safeguards; and
- Periodically evaluate and update their security program.

Best Practices – National Institute of Standards and Technology (NIST)

- Limit information system access to authorized users (Access Control Requirements);
- Ensure that system users are properly trained (Awareness and Training Requirements);
- Create information system audit records (Audit and Accountability Requirements);
- Establish baseline configurations and inventories of systems (Configuration Management Requirements);
- Identify and authenticate users appropriately (Identification and Authentication Requirements);
- Establish incident-handling capability (Incident Response Requirements);
- Perform appropriate maintenance on information systems (Maintenance Requirements);
- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Screen individuals prior to authorizing access (Personnel Security Requirements);
- Limit physical access to systems (Physical Protection Requirements);
- Conduct risk assessments (Risk Assessment Requirements);
- Assess security controls periodically and implement action plans (Security Assessment Requirements);
- Monitor, control, and protect organizational communications (System and Communications Protection Requirements); and

- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

Sanctions

- Title IV aid will be immediately revoked in case of a security breach. Depending upon the severity, institutions may indefinitely lose eligibility to participate in T4.
- $54,789 institutional fine per incident of non-compliance with GLBA.
- $10,000 personal fine – President, Chief Financial Officer, Director of Financial Aid
- ED's latest audit guide has questions regarding the institution's compliance with GLBA. If found unmet, the institution may face penalties.

Recommendations

CREATE INSTITUTIONAL POLICIES

- Barton should add a section to the institutional policies and procedures regarding GLBA.

PUBLISH GLBA INFORMATION ON THE BARTON WEBSITE

- Barton should publish information on the college website regarding GLBA. (See examples from other schools below.)

FORM A TASK FORCE RESPONSIBLE FOR GLBA AND OTHER CYBER-SECURITY REQUIREMENTS

- Much like handling Student Consumer Information, Barton should consider creating a cyber-security team to meet periodically to ensure compliance with all external requirements regarding protecting PII.
  - ✓ GLBA
  - ✓ GDPR
  - ✓ FERPA
  - ✓ HIPPA
  - ✓ FTC – Red Flag Rules

AWARENESS

- The Board of Trustees and Barton's administration should be made aware of federal requirements. Institutional awareness should be raised through training, information-sharing, etc.

References

- https://ifap.ed.gov/eannouncements/Cyber.html
- https://ifap.ed.gov/dpcletters/GEN1518.html
- https://ifap.ed.gov/dpcletters/GEN1612.html
- http://www.uakron.edu/ogc/legal-policies-and-procedures/privacy-practices-and-policies/gramm-leach-bliley-act-glba.dot
- http://technology.pitt.edu/security/gramm-leach-bliley-act
- https://www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/glba

- http://www.nacubo.org/Search_Results_Page.html?q=glba
- http://www.webcastregister.live/2017fsatc_records/viewv2/294/
- http://www.webcastregister.live/2017fsatc_records/viewv2/287/
- https://www.gao.gov/products/GAO-18-121