

Gramm-Leach-Bliley Act

15 U.S.C. §§ 6801-6809

Purdue University
IT-Security and Policy
(Revised November 2005)

Objectives for GLBA Overview

- What is GLBA?
- Why does it apply to Purdue University?
- How does Purdue comply with GLBA?
- What is the penalty if Purdue does not comply?
- GLBA Terms and Definitions
- Additional information sources

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting financial institutions. The law requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information.
- The GLBA is composed of several parts, including the Privacy Rule (16 CFR 313) and the Safeguards Rule (16 CFR 314).

GLBA Compliance with the Privacy Rule

The Federal Trade Commission (FTC) has officially stated that any college or university that complies with the Federal Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g) and that is also a financial institution subject to the requirements of GLBA shall be deemed to be in compliance with GLBA's privacy rules if it is in compliance with FERPA. (16 CFR 313.1)

The FTC has not made a similar exception for an institution of higher education with respect to the Safeguards Rule. Purdue must comply with the Safeguards Rule.

Why does the GLBA Safeguards Rule apply to Purdue?

- Purdue significantly engages in student loan making and provides other financial services. As such, Purdue falls within the definition of “financial institution” under the GLBA and must comply with the laws requirements.
- “Financial Institution” means any institution the business of which is engaging in financial activities.

Examples of Financial Activities That Are Covered by GLBA:

- Student or other loans, including receiving application information, and the making and servicing of such loans
- Collection of delinquent loans
- Check cashing services
- Financial or investment advisory services
- Credit counseling services
- Travel agency services provided in connection with financial services
- Tax planning or tax preparation
- Obtaining information from a consumer report
- Career counseling services for those seeking employment in finance, accounting or auditing

- *Customer Information* is any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.

GLBA Definitions (Continued)

Non-Public Personal Information means personally identifiable financial information that is:

1. Provided by a consumer to a financial institution;
2. Resulting from any transaction with the consumer or any service performed for the consumer; or
3. Otherwise obtained by the financial institution.

The term also includes any list, description, or other grouping of consumers and publicly available information pertaining to them that is derived using any personally identifiable financial information that is not publicly available.

Examples of Nonpublic Personal Information (NPI) Include:

- Social Security Number (SSN)
- Financial account numbers
- Credit card numbers
- Date of birth
- Name, address, and phone numbers when collected with Financial data
- Details of any financial transactions

- The Safeguards Rule requires all financial institutions to develop an information security program designed to protect “customer information.”
- “*Information Security Program*” means the administrative, technical, or physical safeguards used by a financial institution to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

GLBA Safeguards Rule (Continued)

- In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard the customer information in their care.
- “*Affiliate*” means any company that controls, is controlled by, or is under common control with another company.
- “*Service Provider*” means any person or entity that receives, maintains, processes, or otherwise is permitted to access customer information through its provision of services directly to a financial institution.

The objectives of the GLBA Safeguards Rule are to:

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

Purdue's Requirements Under the Safeguards Rule

The Safeguard Rule requires financial institutions to develop an information security program that includes the following:

1. Designate a Security Program Coordinator responsible for coordinating the program;
2. Conduct a risk assessment to identify reasonably foreseeable security and privacy risks;
3. Ensure that safeguards are employed to control the identified risks and regularly test and monitor the effectiveness of these safeguards;
4. Oversee service providers, including selection of appropriate service providers and use of contract language to protect customer information handled by service providers; and
5. Evaluate and adjust the information security program in light of relevant circumstances and changes in the business.

When a Purdue department implements safeguards to protect the security, confidentiality, and integrity of customer information, there are three types of safeguards that must be considered:

1. Administrative Safeguards
2. Technical Safeguards; and
3. Physical Safeguards.

Administrative safeguards include:

- Checking references on potential employees.
- Training employees to take basic steps to properly protect customer information.
- Limiting access to customer information to only those employees who have a business need to see such information.
- Asking every new employee to sign an agreement to follow your department's confidentiality and security standards for handling customer information.

Administrative Safeguards (Continued)

- Instructing and regularly reminding all employees of the legal requirement and of University and departmental policy to keep customer information secure and confidential.
- Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.
- Imposing disciplinary measures for any breaches of policy.
- Referring all requests for customer information to designated individuals who have had safeguards training.
- Recognizing fraudulent attempts to obtain customer information and report to law enforcement agencies.

Physical safeguards include:

- Storing paper records in a locked room, cabinet, or other container.
- Using password-activated screensavers.
- Using strong passwords (at least eight characters long).
- Changing passwords periodically and not sharing passwords or writing them down.
- Ensuring that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods.
- Disposing of customer information appropriately.

Technical safeguards include:

- Storing electronic customer information on a secure server that is accessible only with a password or has other security protections, and is kept in a physically-secure area.
- Maintaining secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
- Avoiding storage of customer information on machines with an Internet connection.

Technical Safeguards (Continued)

- Encrypting sensitive customer information when it is transmitted electronically over networks or stored online.
- Maintaining up-to-date firewalls.
- Using anti-virus software that updates automatically.
- Obtaining and installing software patches promptly.
- Following written contingency plans to address breaches of safeguards.

Guidelines for Providing Secure Data Transmission

- If you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit.
- If you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail.
- If you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.

Guidelines for Secure Disposal of Customer Information

- Hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information.
- Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up.
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information.
- Promptly dispose of outdated customer information.

- Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures.
- Effective security management requires policies and procedures to deal with these failures.

Maintaining Up-to-Date Programs and Controls

- Follow a written contingency plan to address any breaches of physical, administrative or technical safeguards.
- Check with software vendors regularly to obtain and install patches that resolve software vulnerabilities.
- Use anti-virus software that updates automatically.
- Maintain up-to-date firewalls, particularly if using broadband Internet access or allowing employees to connect from home or other off-site locations.
- Provide central management of security tools for employees and pass along updates about any security risks or breaches.

Maintaining Up-to-Date Programs and Controls (Continued)

- Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.
- Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.
- Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

Role of IT Security & Policy in GLBA compliance

- Risk Assessments
- Guidelines for secure computer data
- Educational Materials
- Providing security tools and software
- Providing support for security issues
- Security event response

- The FTC may bring an administrative enforcement action against any financial institution for non-compliance with the Safeguards Rules.
- Penalties for violating Safeguards Rule would likely include equitable damages caused by the loss of privacy, for example, a breach of security resulting in an identity theft.

Information about Purdue's Computing Security Policies

Many of Purdue's existing policies already address some of the compliance issues in the GLBA Safeguards Rule.

- To view Purdue policies, visit <http://www.purdue.edu/policies/index.html> for information about computer security policies including:
 - » Authentication and Authorization
 - » Data Security and Access
 - » Privacy of Electronic Information
 - » Remote Access to IT Resources
 - » Proper Disposal of Electronic Media

Selected University Executive Memoranda

- No. B-50, Terms and Conditions of Employment of Faculty Members:
http://www.purdue.edu/oop/policies/pages/human_resources/b_50.html
- No. B-54, Requesting Social Security Numbers for Educational, Employment and Other Record Keeping Purposes:
http://www.purdue.edu/oop/policies/pages/human_resources/b_54.html
- No. B-55, Terms and Conditions of Employment of Administrative and Professional Staff:
http://www.purdue.edu/oop/policies/pages/human_resources/b_55.html
- No. C-2, Disclosure of University Records: Procedures for Use in Connection with the “Access to Public Records” Law, and in Response to Third-Party Subpoenas:
http://www.purdue.edu/oop/policies/pages/human_resources/c_2.html

Selected University Executive Memoranda (Continued)

- No. C-8, Policy for Security Standard Practice Procedures:
http://www.purdue.edu/oop/policies/pages/records/c_8.html
- C-10, Delegation of Administrative Authority and Responsibility to Officers Reporting to the President of the University:
http://www.purdue.edu/oop/policies/pages/governance/c_10.html
- No. C-34, Data Security and Access Policy Statement:
http://www.purdue.edu/oop/policies/pages/information_technology/c_34.html
- No. C-41, Assignment of Authority and Responsibility for the Retention and Disposal of University Records:
http://www.purdue.edu/oop/policies/pages/records/c_41.html
- No. C-51, University Policy Regarding the “Family Educational Rights and Privacy Act of 1974” (as amended):
http://www.purdue.edu/oop/policies/pages/records/c_51.html

For More Information at Purdue

- ITaP Security and Policy web page: <http://www.itap.purdue.edu/security/>
- Selected Purdue Information Technology Administrative Computing Guidelines or Policies:
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Selected Procedures
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Selected Guidelines
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Best Practices <http://www.itap.purdue.edu/security/policies/>
- Administrative Data Classifications & Information Owners web page:
<http://www.itap.purdue.edu/security/procedures/dataClassif.cfm>
- FERPA Guidelines at Purdue:
<http://www.purdue.edu/Registrar/Records/FERPA/index.htm>

Resources at these sites may alert you to new risks to information security and help those individuals whose information may have been compromised with their next steps.

- The Federal Trade Commission: <http://www.ftc.gov/>
- Additional guidance regarding GLBA is available at: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

For More Information

In addition, the following organizations have information available to help you implement appropriate safeguards for your customer data:

- Computer Security Resource Center, The National Institute for Standards and Technology (NIST):
www.csrc.nist.gov
- Critical Infrastructure Assurance Office (CIAO):
www.ciao.gov
- System Administration, Networking and Security Institute (SANS) - www.sans.org
- The 20 Most Critical Internet Security Vulnerabilities -
www.sans.org/top20.htm

Who to Contact With Questions?

- Contact your manager for specific procedural questions in your area.
- Contact IT Security & Policy for Risk Assessments, educational materials, and help with computer security.
- To contact IT Security & Policy send e-mail to: itap-securityhelp@purdue.edu