

# Financial Modernization Act of 1999, or Gramm-Leach-Bliley Act (GLB) - Law Summary

## DESCRIPTION OF THE LAW

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLB Act, is a federal law that requires financial institutions to take steps to ensure the security and confidentiality of a consumer's (student) records.

Higher education institutions participate in financial activities such as student loans, personal check, and credit card payments; therefore, the Federal Trade Commission (FTC) considers higher education to be a financial institution under the GLB Act.

### How does the law apply to information?

The law requires an information security program with three objectives:

1. Ensure security and confidentiality of consumer (student) information.
2. Protect against any anticipated threats to the security or integrity of such information.
3. Safeguard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.

The law requires an information security program that includes these five required components:

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; 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.
5. Evaluate and adjust the program in light of relevant circumstances and changes in the business.

The law defines safeguard responsibilities of an institution for

1. Administrative - Employee references; training and understanding of the law
2. Physical - Working with, securing and disposal of private information,
3. Technical - Password protected screensaver; continuous change frequency of passwords; security of screen views; rules for communicating private information to others

## **What information does the law protect?**

Customer (student) information is protected, which is any record containing nonpublic, personally identifiable financial information about a consumer (student). This includes paper, electronic, or any form that is handled, or maintained, by the District or District contractors.

Examples of consumer (student) information:

- FERPA standards can be used for names, addresses, and phone numbers, and electronic mail address
- Bank account numbers (protected by GLB)
- Credit Card account numbers (protected by GLB)
- Income, payment, and credit histories (protected by GLB)
- Credit ratings (protected by GLB)
- Date and/or location of birth (protected by GLB)
- Drivers license information (protected by GLB)
- Social Security Number (protected by FERPA and GLB)
- Student loans (Financial Aid) (protected by GLB)
- Tax return (protected by GLB)
- Financial institution information, financial references, loan applications (protected by GLB)

## **GLB Safeguards Checklist:**

1. Turn your computer monitor away from public view.
2. Set up a password protected screensaver on your computer that comes on within at least 15 minutes of inactivity.
3. Use strong passwords (i.e., at least 7 characters in length with a combination of letters and numbers.)
4. Do not write passwords on "post it" notes stick them to your monitor. Use a password that you can remember so you won't have to write it down.
5. Change passwords periodically.
6. Change your password immediately if you think anyone else knows your password.
7. Do not give your password to anyone. (Note: Only in rare situations will an IT staff member need to know your password to fix a reported problem. After the problem has been resolved, you must change your password so that only you know it.)
8. Do not repeat credit card numbers over the phone where other unauthorized people can over hear the number.
9. Cardholder receipts should display no more than the last four digits of the credit card number (paper or electronic).

10. GroupWise email should NOT be used to send any confidential/sensitive information such as bank or credit card numbers, grades, etc.
11. Do not allow students to send their credit card number to your GroupWise e-mail address. GroupWise email should NOT be used to receive any confidential/sensitive information such as bank or credit card numbers, grades, etc.
12. Do not store district information on the "C" drive of your computer. It should be stored on a secure district network drive, e.g., U:, P:, etc.
13. Do not leave sensitive paperwork or loan applications open on your desk if doing so would allow it to be accessible/visible to unauthorized people.
14. Keep rooms and file cabinets where customer information is kept locked at all times and limit access to authorized employees (especially workspaces in public areas).
15. Shred customer information recorded on paper or store it in a secure area until approved disposal vendor service picks it up (remember your note pads and scratch paper).
16. Dispose of outdated customer information within record retention policies.
17. Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods.

A more detail review of the law can be found on the District Web Site at the following link:  
<http://www.dcccd.edu/Employees/Policy+and+Procedures/IPSP/IPSP+Links.htm>