

The Community College of Baltimore County

**Gramm-Leach-Bliley Act
Information Security Plan**

Updated June10, 2005

Table of Contents

- 1. The Gramm-Leach-Bliley Act – What is it?**
- 2. Privacy of Consumer Information Rule (Privacy Rule)**
- 3. Safeguarding of Consumer information Rule (Safeguards Rule)**
 - 3.1. Gramm-Leach-Bliley Compliance Team
 - 3.2. Administrative Safeguards
 - 3.2.1. Criminal Background Checks
 - 3.2.2. Confidentiality Agreements
 - 3.2.3. Employee Management and Training
 - 3.2.4. Service Providers
 - 3.3. Physical Safeguards
 - 3.4. Technical Safeguards
 - 3.4.1. Information Systems – Storage of Data
 - 3.4.2. Information Systems – Transmission of Data
 - 3.4.3. Information Systems – Disposal of Data
 - 3.4.4. Information Systems – Managing System Failures
- 4. Glossary of Terms**
 - 4.1 CISP – Cardholder Information Security Program
 - 4.2 Customer information
 - 4.3 “Digital Dozen”
 - 4.4 Directory information
 - 4.5 Information security program
 - 4.6 FERPA – Family Education Rights and Privacy Act
 - 4.7 Nonpublic personal information
 - 4.8 Service provider

Appendices

- | | |
|------------|-------------------------------------------------------|
| Appendix A | Federal Register 16 C.F.R. Part 313 – Privacy Rule |
| Appendix B | Family Educational Rights and Privacy Act (FERPA) |
| Appendix C | Student Records Policies and Procedures |
| Appendix D | Federal Register 16 C.F.R. Part 314 – Safeguards Rule |
| Appendix E | Employee Confidentiality Agreement |
| Appendix F | Banner Confidentiality Agreement |
| Appendix F | Record Retention Policy |

1. The Gramm-Leach Bliley Act – What is it?

The Gramm-Leach-Bliley Act (GLB), enacted in 2000, requires financial institutions to take steps to ensure the security and confidentiality of customer records such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers.

The GLB Act defines “financial institution” as any institution engaging in financial activities enumerated under the Bank Holding Company Act of 1956, including “making, acquiring, brokering, or servicing loans” and “collection agency services”. Because higher education institutions participate in financial activities, such as making Federal Perkins Loans, FTC regulations consider them financial institutions for GLB purposes.

The GLB Act addresses specific requirements regarding the privacy and safeguarding of customer information.

2 Privacy of Consumer Information Rule (Privacy Rule)

The Privacy Rule, found at 16 C.F.R Part 313 of the Federal Register (Appendix A), addresses concerns relating to consumer financial privacy. Under regulations promulgated in May 2000, colleges and universities are deemed to be in compliance with the privacy provisions of the GLB Act if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). The Family Educational Rights and Privacy Act may be found in Appendix B, and may be viewed on the CCBC website: <http://www.cbcmd.edu/ferpa/index.html>

The Community College of Baltimore County (CCBC) maintains strict compliance with the provisions of FERPA, regarding access, disclosure and confidentiality of customer records. “Student Records Policies and Procedures”, published in compliance with section 99.6 of FERPA, address the following areas:

- Type, Locations and Custodians of Education Records
- Definitions
- Procedure to Inspect Education Records
- Recorded Copies and Fees
- Amendment of Education Records
- Disclosure of Education Records
- Record of Requests for Disclosure
- Directory Information
- Right of Complaint

“Student Records Policies and Procedures” may be found in Appendix C, and may be viewed on the CCBC Website: <http://www.cbcmd.edu/ferpa/policies.html>

3 Safeguarding of Consumer Information (Safeguards Rule)

The Safeguards Rule, found at 16 C.F.R. Part 314 of the Federal Register (Appendix D), deals with the responsibility of financial institutions to ensure the security and confidentiality of consumer financial information. The plan outlined in this document deals with administrative, technical and physical safeguards put into place at CCBC to

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats to the security of such information; and
- Guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

3.1 Gramm-Leach-Bliley (GLB) Compliance Team

The CCBC GLB Compliance Team was formed in January 2004, to oversee the safeguarding of consumer information. The team includes representatives from all areas of the college that deal with financial customer information.

Membership is as follows:

Gail Baldwin (Chair)	Finance Manager
Diane Drake	Director of Admissions – Catonsville Campus
Mark Gay	Director of Financial Aid – Dundalk Campus
Jeff Hagen	Chief of Public Safety
Mildred Singleton	Director of Human Resources
Terry Hirsch	Director of Planning Research and Evaluation
Wally Knapp	Sr. Director of Technology Services
Anne Lefter	Director of Performing Arts
Lynn MacLaughlin	Director of Records & Registration – Essex Campus
James Malm	Chief Administrative Officer – Continuing Education & Economic Development
Pat Mohr	Director of Student Finance
Chris O’Kane	Sr. Director for Banner Applications & Database Management
Jim Stoecker	Manager, Bookstore – Essex Campus

The GLB Compliance Team will meet quarterly after the GLB Information Security Plan is in place, and is charged with:

- Implementing the GLB Information Security Plan, which includes administrative, physical and technical safeguards
- Identifying and assessing risks to customer information in each relevant area of the college
- Evaluating the effectiveness of the existing safeguards in the security plan for controlling the identified risks
- Regularly monitoring and testing the security program
- Selecting appropriate service providers and contracting with them to implement safeguards
- Adjusting the security program in light of relevant circumstances, including changes in the College's business operations, or the results of testing and monitoring safeguards

3.2 Administrative Safeguards

Members of the GLB Compliance Team are administratively responsible for sharing safeguarding compliance guidelines within their respective areas. Managers in those areas are expected to identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. CCBC has instituted the following administrative safeguards to ensure the security and confidentiality of its customer information:

3.2.1 Criminal Background Checks

CCBC may perform a criminal background check on any employee or applicant if the applicant or employee will have access to sensitive customer financial information and CCBC has a reasonable basis to believe that a criminal background check would be in the best interest of the College

3.2.2 Confidentiality Agreements

At orientation, all full time benefit eligible employees and adjunct faculty are required to sign an agreement stating that they will follow CCBC's confidentiality and security standards for handling customer information (see Appendix E). Managers are responsible for ensuring that temporary hourly and student employees, who have access to confidential information, also sign a confidentiality agreement, when they begin their employment.

Employees must also sign a confidentiality agreement (see Appendix F) prior to being given access to the College's Information System (Banner)

3.2.3 Employee Management and Training

CCBC managers in relevant areas are responsible for training employees to take the following basic steps to maintain the security, confidentiality and integrity of customer information.

- All benefit eligible employees are trained to maintain the physical safeguards outlined in the “Physical Safeguards” section of this document
- All benefit eligible employees are trained to comply with FERPA guidelines discussed in the Privacy Rule section of this document.
- Employees are encouraged to use the “Workstation Security Options” outlined below when leaving their workstation:
 - Log off completely when leaving your workstation, so that unauthorized persons cannot gain access to the CCBC network and systems using your ID.
 - If you do not log off completely and are running Windows XP, use the following procedure to lock your workstation: press Ctrl/Alt/Delete; click on “Lock Workstation”; the Novell locked panel will pop up and the PC is locked out of the network until you press Ctrl/Alt/Delete once again; key in your password as directed, press OK and you are back to your initial screen.
- Temporary hourly and student employees, who have not received safeguards and FERPA training, are instructed to refer calls or other requests for customer information to designated individuals who have had the training.
- Employees are instructed to report any fraudulent attempts to obtain information to the Office of Public Safety, who will report it to the appropriate law enforcement agency.
- To the extent possible, access to customer information at CCBC is limited to employees who have been trained and have a business reason for seeing it.

3.2.4 Service Providers

CCBC routinely reviews its third party service providers, to ensure that they comply with safeguarding guidelines. The College has received compliance agreements from the following service providers:

EdFund
ELM Resources
FACTS Tuition Management Co.
National Student Clearinghouse
Sallie Mae

3.3 Physical Safeguards

The following physical safeguards have been implemented at CCBC, to ensure the confidentiality of consumer information.

- Rooms and/or file cabinets containing paper records with confidential customer information are to be locked when unattended
- Access to campus Bursar's Offices, containing financial documents including credit card information, is limited to Bursar staff only. Staff access is controlled by keypad or magnetic card.
- Access to campus Computer Centers is restricted to permanent computer staff only. The centers are locked at all times and access is by key only.
- Paper documents containing confidential customer information, no longer needed, are shredded or placed in recycle bins, which are locked until the recycling service picks up the contents of the bins.
- Retention and disposal of records containing nonpublic information is done in accordance with the College's Record Retention Policy, approved by the Board of Trustees (see Appendix G). The Record Retention Committee is responsible for overseeing the Record Retention Policy.

3.4 Technical Safeguards

The GLB Compliance Team and the Information Technology Services (ITS) Department are expected to identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information in information systems, that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. CCBC has instituted the following technical safeguards to ensure the security and confidentiality of its customer information throughout its life cycle (i.e., from data entry to data disposal):

3.4.1 Information Systems - Storage of Data

To the extent possible, data storage areas are protected against destruction or potential damage from physical hazards. Data is locked in the campus computer centers, with access limited to authorized personnel. The computer centers are protected with new air conditioning units, and diesel generators to protect against disaster.

Electronic customer information is stored on secured servers. All servers are password protected, and located in locked areas within the ITS Department.

Sensitive customer data is never stored on machines with direct Internet connectivity.

Secure backup media is maintained, and archived data is kept secure by storing off-line or in physically secure areas. Currently CCBC uses four locations to store backup data files; the safe in H204 (Catonsville), the safe in K Building (Catonsville), the computer center at Dundalk and the computer center at Essex. Data is rotated daily in locked suitcases.

3.4.2 Information Systems – Transmission of Data

The Visa USA Cardholder Information Security Program (CISP) defines a standard of due care and enforcement for protecting sensitive information. Its primary focus is the e-commerce acceptance channel, and is primarily built upon the “Digital Dozen” list of twelve basic security requirements with which all Visa payment systems constituents must comply. CCBC has taken the following steps to ensure compliance with the “Digital Dozen”.

1. Install and maintain a working firewall to protect data – CCBC has a firewall in place out to the Internet. A redundant unit (a stand-alone piece of hardware) has been installed as a “hot spare”. A firewall is also installed between the administrative and student segments of the network
2. Keep security patches up to date – Security patches are constantly updated, tested, and modified according to the latest industry standards.
3. Protect stored data – Campus computer centers remain locked at all times; data is stored in a secondary safe in the K Building at Catonsville; an alternative storage location at Essex has been identified and backup tapes are cycled and sent there daily.
4. Encrypt data sent across public networks – CCBC utilizes Secure Socket Layer (SSL) for encrypting critical data. Virtual Private Network (VPN) is in use, where necessary, for selected staff to access records. Encrypted VPN is utilized for wireless access via laptops on campus.
5. Use and regularly update anti-virus software – McAfee anti-virus software is installed on all campus desktop computers. Updated virus signatures are received daily (Monday through Friday) and are sent out via the Zenworks network to all desktops at the point of sign-on. All computers are automatically shut down at 11:00pm every evening, forcing users to receive the updated virus on their machines at the point of sign-on.
6. Restrict access by “need to know” – Within the ITS staff, access to data is limited to only those who need to see it.

Gramm-Leach-Bliley Act Information Security Plan

7. Assign unique ID to each person with computer access – Each user has a unique user ID and password. CCBC’s policy is to disconnect users from the system if it has been determined that they have shared their ID and password. GLOPASS software has been installed, to force employees to change their passwords every 180 days. Employees are able to change their passwords more frequently, if they desire. Passwords are given to individual users only, not to departments.
8. Don’t use vendor-supplied defaults for passwords and security parameters – Vendor-supplied defaults are never used. All passwords are changed during the installation of products.
9. Track all access to data by unique ID – user ID is used to limit access to specific parts of the administrative system. Access is limited on a “need to know” basis.
10. Regularly test security systems and processes – Plans for a system security test are tentatively scheduled for summer or fall 2005.
11. Implement and maintain an information security policy – The GLB Information Security Plan includes CCBC’s information security policies.
12. Restrict physical access to data – Campus computer centers are restricted, keyed, and only accessed by permanent ITS staff members.

3.4.3 Information Systems – Disposal of Data

The ITS Department retains and disposes of records, in accordance with the College’s “Record Retention Policy”.

Reports and paper documents containing nonpublic personal information is shredded. A high-speed shredder has been purchased to handle the shredding of large reports.

All data is erased when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information.

Effective disposal of hardware occurs after completion of its useful life cycle.

The ITS Service and Support Manager maintains a comprehensive inventory of computers for the College.

3.4.4 Information Systems – Managing System Failures

CCBC effectively manages system security, including the prevention, detection and response to attacks, intrusion or other system failures. The following programs and controls have been implemented:

CCBC regularly monitors software vendors, to obtain and install patches that resolve software vulnerabilities.

Anti-virus software is utilized and updated automatically.

Up-to-date firewalls are maintained. CCBC currently has two firewalls to the Internet, and a separate firewall between the administrative and student segments of the network.

One ITS staff member is responsible for informing management of any security risks or breaches. Breaches of physical safeguards are reported to the appropriate law enforcement agency, as soon as they are detected.

The appropriate steps have been taken to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. All customer data is backed up nightly, if stored on the central drive (H drive).

The College's Disaster Recovery Plan also addresses the management of system failures in the event of a disaster affecting one or more campus.

4 Glossary of Terms

4.1 CISP - Cardholder Information Security Program – This Visa program defines a standard of due care and enforcement for protecting sensitive information. Its primary focus is the e-commerce acceptance channel, and is primarily built upon the “Digital Dozen” list of twelve basic security requirements with which all Visa payment systems constituents must comply. CCBC regularly monitors its compliance with the “Digital Dozen” requirements.

4.2 Customer information – any record containing nonpublic personal information about a customer or financial institution, whether in paper, electronic, or other form, that is handled or maintained on behalf of the college or its service providers.

4.3 Digital Dozen – list of twelve basic security requirements with which all Visa payment system constituents need to comply.

4.4 Directory information – (FERPA definition) information contained in an education record of a student, which would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended.

Gramm-Leach-Bliley Act
Information Security Plan

4.5 Information security program – the administrative, technical, or physical safeguards the college uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

4.6 FERPA – The Family Education Rights and Privacy Act – Amended in 1974, the Act affords students certain rights of privacy and inspection with respect to their education records. It allows colleges to disclose personally identifiable information in a student's education record under certain circumstances without the consent of the student. Furthermore, FERPA permits colleges to disclose, upon request, directory information, without the consent of the student, unless the student has otherwise directed the college in writing.

4.7 Nonpublic personal information – (as defined in 16 CFR Part 313.3(n) (1)) “personally identifiable financial information; and 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.” An example for CCBC would be information that a student provides on the Free Application for Federal Student Aid (FAFSA).

4.8 Service provider – any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to a financial institution.