BAY MILLS
Community College

Policy Number and Title:	**100.114 BMCC Gramm-Leach Bliley Act (GLBA) Financial Information Security Policy**		
Approval Authority:	BMCC Board of Regents	**Date Effective:**	07/25/2023
Responsible Office:	Information Technology	**Responsible Office Contact:**	Chief Information Officer

1. **POLICY STATEMENT/REASON FOR POLICY**

   To comply with the Gramm-Leach-Bliley Act (GLBA) which safeguards financial information. The Gramm-Leach-Bliley Act (Public Law 106-102) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data (16 CFR 314). The Federal Trade Commission considers Title IV-eligible institutions that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 CFR 313.3(k)(2)(vi)).

2. **ENTITIES AFFECTED BY THIS POLICY**

   All GLBA Relevant Departments.

3. **WHO SHOULD READ THIS POLICY**

   All GLBA Relevant Department employees.

4. **WEB SITE ADDRESS FOR THIS POLICY**

   -This URL for this policy is at:
   http://www.bmcc.edu/about-bmcc/governance-administration/college-policies

5. **FORMS/INSTRUCTIONS**

   No forms required.

6. **HISTORY**

   -Created: 07/25/2023.
   -Next Review Date: 07/25/2026.
   -BMCC reserves the right to revise policies at any time.

7. THE POLICY

BMCC GRAMM-LEACH BLILEY ACT (GLBA)

FINANCIAL INFORMATION SECURITY POLICY

I. PURPOSE/POLICY:

The Gramm-Leach-Bliley Act (Public Law 106-102) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. (16 CFR 314) The Federal Trade Commission considers Title IV-eligible institutions that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 CFR 313.3(k)(2)(vi).

Under BMCC's Program Participation Agreement with the Department of Education and the Gramm-Leach-Bliley Act, schools must protect student financial aid information, with particular attention to information provided to institutions by the Department or otherwise obtained in support of the administration of the federal student financial aid programs. (16 CFR 314.3; HEA 483(a)(3)(E)) and HEA 485B(d)(2))

The Federal Trade Commission's Safeguards Rule implements the security provisions of the Gramm-Leach-Bliley Act (GLBA). The Safeguards Rule requires financial institutions, which includes colleges and universities that are significantly engaged in providing Financial Services, to protect the security, confidentiality, and integrity of customer financial records, including non-public personally identifiable financial information. To ensure this protection, the GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical and physical safeguards (Reference 16 CFR § 314.1(a)).

II. SCOPE:

This Policy applies to all BMCC departments and may also apply to the College's Related Entities under certain circumstances as defined in this Policy. Thus, any BMCC College department that collects, stores or processes Covered Data must comply with this policy. This policy is in addition to any other College policies that are required pursuant to federal privacy law and regulations (e.g. Family Educational Rights and Privacy Act (FERPA)).

III. REASON FOR POLICY:

To ensure that individuals and departments that access or utilize Covered Data understand their responsibility with respect to GLBA compliance.

IV. WHO SHOULD READ THE POLICY:

A. Any individual or department that has access to Covered Data including but not limited to the following (GLBA Relevant Departments):
   - Enrollment employees (Recruiting, Admissions, Applications Processing, Registrar, Financial Aid).
   - Finance, Cashier (and all collection points), Accounting, Accounts Payable, Vendor Management, Customer Management, Grants Management.
   - Human Resources.
   - Adult and Continuing Education and Similar Programs and Offices.
   - Student Affairs.
   - Academic Affairs.
   - Information Technology.

V. POLICY OBJECTIVES:

A. Protect the security and confidentiality of Covered Data.

B. Protect against anticipated threats or hazards to the security or integrity of Covered Data; and,

C. Protect against unauthorized access to or use of Covered Data that could result in substantial harm or inconvenience to any Customer.

VI. DEFINITIONS:

"College" means the Bay Mills Community College.

"Covered Data" is defined as:

(i) non-public personal financial information about a customer; and,

(ii) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information.

Covered Data is subject to the protections of GLBA, even if the Customer ultimately is not awarded any financial aid or provided with a credit extension.

Covered Data examples include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of students with outstanding loans).

Covered Data includes such information in any form, including paper and electronic records.

"BMCC" and "College" interchangeably means the Bay Mills Community College.

"Customer" means any individual (student, parent, faculty, staff, or other third party with whom the College interacts) who receives a Financial Service from the College for personal, family or household reasons that results in a continuing relationship with the College.

"Financial Service" includes offering or servicing student and employee loans, receiving income tax information from a student or a student's parent when offering a financial aid package, engaging in debt collection activities, and leasing real or personal property to individuals for their benefit.

"Related Entities" means the following types of entities and their subsidiaries, if legally separate from the College and unless otherwise indicated: auxiliary enterprise corporations, college associations, student services corporations, childcare centers, performing arts centers, and art galleries.

"Service Provider" means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Data information through its direct provision of services to the College.

VI. GLBA REQUIREMENTS:

The GLBA requires that the College (i) designate an employee(s) to coordinate the Program, (ii) identify internal and external risks to the security and confidentiality of Covered Data and evaluate current safeguards, (iii) design and implement safeguards to control the identified risks and regularly test and monitor the effectiveness of these safeguards, (iv) oversee Service Providers and contracts, and (v) evaluate the information security program.

A. GLBA Program Coordinator Designation:

The College President shall designate an appropriate individual to serve as the GLBA College Program Coordinator, who will administer BMCC's Information Security Program and serve as the primary College resource for addressing issues related to the GLBA Safeguards Rule and disseminating relevant information and updates.

The BMCC President has designated the BMCC Chief Information Officer to be the GLBA College Program Coordinator.

B. The GLBA College Program Coordinator shall verify that the institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4 (b): (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

C. Identification of Risks and Risk Assessment:

BMCC recognizes that there are both internal and external risks associated with the protection of Covered Data. These risks include, but are not limited to:

- Unauthorized access to Covered Data.
- Compromised system security because of system access by an unauthorized person.
- Interception of Covered Data during transmission.
- Loss of data integrity.
- Physical loss of Covered Data in a disaster.
- Errors introduced into the system.
- Corruption of data or systems.
- Unauthorized transfer of data by an Authorized User
- Unauthorized requests for Covered Data.
- Unauthorized access to hard copy files or reports containing Covered Data.
- Unauthorized transfer or release of Covered Data by third parties contracted by the College.
- Unauthorized disposal of Covered Data; and
- Unsecured disposal of Covered Data.

BMCC also recognizes that the above may not be a complete list of risks associated with the protection of Covered Data. Since technology changes over time, the possibility of new risks may arise. BMCC's data owners and custodians will actively seek to identify and address all potential technology security risks associated with Covered Data. In addition, the IT Department shall incorporate continuous

monitoring and identification of security risks and controls into its Annual Risk Assessment/Internal Control Review process.

D Safeguarding Program Components:

a. Employee Training and Management

(i). All BMCC employees in departments that collect, access, retain, transmit or dispose of Covered Data (GLBA Relevant Departments) will receive a copy of this Information Security Policy. Each department director covered by this Information Security Policy is responsible for ensuring that all employees under their direction receive this document and for clarifying how the Information Security Policy is applicable to the employees in their department. The Department Heads shall ensure that each department director is aware of this responsibility.

(ii). On an ongoing basis, each department head shall ensure that all new employees in their department, whether new hires or transfers, receive a copy of this Information Security Policy as part of the orientation to the department. The GLBA College Program Coordinator will arrange for training of the various groups impacted by the GLBA Safeguards Rule throughout the College, as needed, on an ongoing basis.

b. Information System Security

(i). Access to Covered Data through College networks and stand-alone systems shall be limited to those employees who have a business reason to have such information per IT Security Procedure requirements. Only employees with the need to have access to certain Covered Data shall be granted access to that data or be authorized to collect such data from Customers. All databases and imaged documents containing Covered Data must be appropriately protected, including use of password or other authentication, encryption, and other access restrictions as appropriate.

(ii). While the College utilizes industry-standard protocols and cybersecurity technologies, including firewalls, intrusion prevention, encryption, anti-malware, email security and restricted physical access to its data centers to protect its digital assets, everyone's participation is required, in consultation with BMCC and College information technology departments, to ensure that reasonable and appropriate steps are taken to protect Covered Data and to safeguard the integrity of records in storage and transmission. These steps include maintaining operating systems and applications, applying security-related updates in a timely manner after appropriate testing and reviewing overall protections on an ongoing basis.

(iii). All Covered Data shall be handled with care and scrutiny and shall be protected and controlled, including but not limited to storage on college servers and cloud storage behind firewalls where applicable. All College information security software and hardware protections shall be maintained with vendor support at current or higher levels. Sensitive data discovery and data loss prevention tools shall be utilized in areas of high risk to ensure that Covered Data is identified and protected as required.

(iv). At all times, Covered Data shall be maintained in a manner consistent with college policies and procedures. Encryption technology should be used for both storage and transmission of all Covered Data where possible. Encryption of Covered Data on mobile devices is required per IT Security Procedures.

(v). Policies shall be periodically reviewed and modified, and new policies developed as needed, to define required security for College information systems.

c. Safeguarding Paper and Electronic Records

Access to Covered Data shall be limited to those employees who have a business reason to have such information per IT Security Procedure requirements. Whether this information is stored in hard copy form or electronically, employees must exercise appropriate care for its safekeeping by following these guidelines:

i. Safeguarding Paper Information

a. Secure Covered Data by locking file cabinets and offices when not in use.
b. Do not leave Covered Data unattended and unsecured.
c. Access to Covered Data shall only be granted to those who need such access.
d. Comply with other applicable College policies and procedures including, but not limited to, BMCC's Records Retention Schedule.

ii. Safeguarding Electronic Information

a. Password-protect computers and systems with access to Covered Data and log off computers and systems when access to Covered Data is no longer needed. Shut down and turn off computers at the end of each day where possible (when working remotely, this may not be possible).
b. Do not leave Covered Data unattended and unsecured.
c. Access to computers and systems shall only be granted to those who need such access.
d. Encrypt Covered Data when transmitting or storing it electronically.
e. Monitor systems for actual or attempted attacks, intrusions, or other systems failures.
f. Comply with all other applicable College policies listed at the end of this policy.
g. Periodically conduct a Cybersecurity Assessment and address any concerns.

d. Disposal of Records Containing Covered Data

Stored records containing Covered Data shall be maintained only until they become inactive or are no longer required under applicable rules and regulations. When no longer active or required, records shall be destroyed or retired in accordance with BMCC's Records Retention Schedule governing the disposition of such records. Paper records that are no longer required to be kept by the College shall be shredded at the time of disposal. Electronic documents shall be deleted, and magnetic media shall be erased.

The designated Records Retention Officer at each College Department is responsible for administering a records management program and should be consulted with any questions about the disposition status of records.

E. Oversight of Service Providers and Contracts:

The GLBA Safeguards Rule requires that the College take reasonable steps to select and retain Service Providers who will maintain safeguards to protect Covered Data. Appropriate steps shall be taken to ensure that all relevant contracts include a privacy clause, and that all existing contracts follow GLBA.

F. Program Review and Revision:

This policy is subject to review and revision to ensure compliance with current and future laws and regulations. Except for modifications, supplements or updates necessitated by changes in law, regulations, or administrative requirements, or to ensure consistency with other College policies, any proposed amendments to this Policy must be approved by the BMCC Board of Regents. The BMCC IT Department will be responsible for the periodic review of this Policy.

G. Application To Related Entities:

1. Any Related Entity that provides a Financial Service or assists the College with the administration of a Financial Service shall comply with this policy as follows:
    a. Related Entities that maintain or distribute Covered Data relating to a Financial Service on or through a College server or other technology under college control, or which assist the College with the administration of a Financial Service shall be deemed to be part of their supported College, solely for purposes of compliance with this policy.
    b. Related Entities that are subject to GLBA but maintain and/or distribute Covered Data relating to a Financial Service independent of any College-controlled technology and do not assist the College or a College with the administration of a Financial Service, shall adopt their own policies consistent with the requirements of GLBA and this policy, including without limitation regarding information system security, the training of employees, and safeguarding of information.

Related Policies:

100.104	**BMCC Records Retention Policy, Revised** 07/14/2023
100.110	**BMCC FERPA Compliance Policy,** Revised 03/18/2022
200.111	**BMCC Student Billing Policy,** Revised 10/06/2021
300.805	**Use of Communications Systems,** Revised 06/18/2021
400.400	**Student Handbook,** Version 2018
500.101	**500.101 BMCC Disaster Recovery Policy,** Revised 09/17/2021