Mott Community College
GLBA Required Information Security Program
June 2023

Overview: This document summarizes the Mott Community College (the "college's") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the college intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the college's policies and procedures enumerated below and is in addition to any college policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: The college's Chief Technology Officer is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the college to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or their designees.

Scope of Program: The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the college, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the college or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the college, (ii) about a student or other third party resulting from any transaction with the college involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program:

1. Risk Identification and Assessment. The college intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the college's operations, including:

- *Employee training and management*. The Program Officer will coordinate with representatives in the college's Human Resources, Student Success Services, and Financial Aid offices to evaluate the effectiveness of the college's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the college's current policies and procedures in this area as outlined in the Mott Community College Financial Aid Policies and Procedures manual and the Records Office student policies.

- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives of the college's Information Technology Services division to assess the risks to nonpublic financial information associated with the college's information systems, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information. This evaluation will include assessing the college's current policies and procedures relating to the college's Acceptable Use Policy and Information Security Policy. The Program Officer will also coordinate with the college's Information Technology Department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing, and Responding to Attacks*. The Program Officer will coordinate with the college's Information Technology Services division to evaluate procedures for and methods of detecting, preventing, and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the Information Technology Services division the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the college.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper, or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The Program Officer shall coordinate with those responsible for the third-party service procurement activities among the Information Technology Services division and other affected departments to raise awareness of and to institute methods for, selecting and retaining only those service providers that are

capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officer will work with the legal counsel selected by the college to develop and incorporate standard, contractual protections applicable to third-party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the legal counsel selected by the college. These standards shall apply to all existing and future contracts entered into with such third-party service providers. The college's Business Office will develop and send form letters to all covered entities requesting assurances of GLBA compliance.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the college's operations or other circumstances that may have a material impact on the Program.