Madison Adult Career Center (MACC)
Gramm—Leach—Bliley Act (GLBA) Policy and Procedures

Gramm—Leach—Bliley Act (GLBA) Required Information

Overview: MACC is required to maintain comprehensive written security procedures, responsibilities and guidelines as mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). This law requires that MACC (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 (students). The Program is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: The District Administration designates the Technology Department, Adult Education Director, Assistant Director and MACC's Financial Aid personnel who shall be responsible for coordinating and overseeing the Program. MACC's Financial Aid Office will 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 MACC's Financial Aid Office.

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 District, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the District 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 Institution, (ii) about a student or other third party resulting from any transaction with the District 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 District 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 Officers will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- *Employee training and management.* The Program Officers will coordinate with representatives in the District's Administrative offices to evaluate the effectiveness of the District'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 Institution's current policies and procedures in this area, including the Adult Student Catalog, District Employee Handbook, and Employee Training Requirements.

- *Information Systems and Information Processing and Disposal.* The Program Officers will coordinate with representatives of the District's Technology Department to assess the risks to

nonpublic financial information associated with the District'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 District's current policies and procedures relating to the Acceptable Use, Information Security, Public Records, Student Records, and Confidentiality Policies. The Program Officers will also coordinate with the District's 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 Officers will coordinate with the District's Technology Department 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 Officers may elect to delegate to a representative of the Technology Department the responsibility for monitoring and participating in the dissemination to students and the USDOE of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the District.

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 Officers 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 Officers shall coordinate with those responsible for the third party service procurement activities among the Technology Department 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 Officers will work with the District Administration to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

4. Adjustments to Program. The Program Officers are 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 District's operations or other circumstances that may have a material impact on the Program.

Updated January 5, 2024, SLP