Monroe County Community College

Data Security Procedure

Procedure Type: District Procedure

Procedure Title: Data Security Procedure

This Procedure Affects: Administrators, Faculty, Staff

Purpose: Monroe County Community College is committed to protecting its data. Data Storage environments including Cloud Storage are useful in many ways. However, there are inherent risks relative to security, copyright, privacy, and data retention. Unlike data stored on-premise, when documents are saved in Cloud Storage environments, the College must identify the appropriate administrative and access controls for the stored data. This procedure notes best practices and applies to all MCCC employees and affiliates that store the College data classifications outlined in this procedure. The Data Security Procedure falls under Computer and User Policy 6.50.

Scope: This procedure applies to all persons accessing MCCC data on-premise and/or using 3rd-party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by Monroe County Community College, all consultants or agents of the College, and any parties who are contractually bound to handle data produced by and in accordance with college contractual agreements and obligations. Additionally, all persons sharing MCCC data with external or 3rd-party entities must engage in a data sharing agreement. This agreement must minimally include the language outlined in the college's Data Sharing Agreement Template. All data sharing agreements must be reviewed and signed by the Director of Institutional Effectiveness and Chief Data Officer.

Compliance with Legal and Regulatory Requirements: The College has many federal laws that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), RI General Laws 11-49.3 (Identify Theft Protection Act) and 5-37.3 (Confidentiality of Health Care Communications and Information Act), and the Health Insurance Portability and Accountability Act (HIPPA). These federal laws must also be outlined in the data sharing agreement between MCCC and any external/3rd-party entity (as required by the Data Sharing Agreement Template).

Definitions

<u>Data Classifications</u>:

Protected Data - Under state law, Personally Identifiable Information (PII) means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format:

- Social security number
- Driver's license number, state identification card number, or tribal identification number

- Account number, credit card number, or debit card number, with or without any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account
- Medical or health insurance information
- E-mail address with any required security code, access code, security Q&A, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Sensitive Data – Data not meant for public distribution but not classified as Protected Data (i.e., internal policies, internal memos, Intranet information, grades, grade point average (GPA), courses taken or not taken, an individual's degree information)

Public Data – Data meant for public distribution (i.e., external website, public relations materials, degrees offered by the institution, etc.)

The MCCC Data Governance Board or Chief Data Officer may review and change the classification of data as needed.

Storage Classifications:

Cloud Storage – Cloud infrastructure provisioned for open use by the general public (i.e., Dropbox, Microsoft OneDrive - Personal, Google Docs - Personal, etc.)

College System on Premise – Private on-premise Infrastructure provisioned for the exclusive use of Monroe County Community College (i.e., Network Drives, Student Information System (Ellucian Colleague), Finance System, HR System, etc.)

College System Cloud-based – Cloud Infrastructure provisioned for the exclusive use of Monroe County Community College (i.e., Microsoft O365, Colleague, Ethos, Brightspace, etc.)

Local Storage – Personal or MCCC devices not connected to a network-controlled infrastructure (i.e., USB drives, laptops, desktop computers, etc.)

Policy Guidelines: The following guidelines note the permitted and prohibited storage systems for the data classifications outlined in this policy. The following categories do not change, regardless of media type. Paper documents containing protected or sensitive data are not to leave campus and must be stored in a secure location.

Data Classification	**Cloud Storage**	**College System on Premise**	**College System Cloud-based**	**Local Storage**
Protected Data	Prohibited	Permitted	Permitted with Encryption	Prohibited
Sensitive	Prohibited	Permitted	Permitted with Encryption	Prohibited
Public	Permitted	Permitted	Permitted	Permitted

Self-provisioned, personal cloud service accounts may not be used for protected or sensitive data. Regardless of the classification of data used, cloud service accounts must comply with college licensing and legal requirements.

When protected or sensitive data is downloaded locally, it is saved by default to the Downloads folder. After it is downloaded, it must be moved to a secure location and is not to remain in your Downloads folder.

If transporting protected or sensitive data across campus using a portable thumb drive, protected or sensitive data must be removed from the portable thumb drive after it has reached its secure destination.

Data Sharing:

Data sharing of any protected data must be reviewed by the Data Governance Board. The Data Governance Board is charged with reviewing any request for data sharing and must approve of what protected, sensitive, and public information will be allowed to be shared with the 3rd-party.
As stated above, all persons sharing MCCC data with external or 3rd-party entities must engage in a data sharing agreement. This agreement must minimally include the language outlined in the college's Data Sharing Agreement Template. All data sharing agreements must be reviewed and signed by the Director of Institutional Effectiveness and Chief Data Officer. The data sharing agreement will outline the 3rd-party obligation to follow best practices to protect the shared data from being compromised.

As required by the college's Data Sharing Agreement Template, data must be encrypted when being transferred to and from a 3rd-party storage solution. Clear text transfers of any data, including public data, is not permittable. The method for transferring data must be approved by the Chief Information Officer upon review of the data sharing agreement and any service agreements. Upon termination of any agreement that transfers college data, the 3rd party must immediately delete the data that was transferred. Also required by the college's Data Sharing Agreement Template, MCCC will establish a required timeframe in which shared data must be deleted by the receiving 3rd-party.