Monroe County Community College
Information Security Plan

Policy Type: District Policy

Policy Title: Information Security Plan

Who Does the Policy Affect: Administrators, Faculty, Staff, and Students

I. Purpose

The purpose of this document is to define the specific policies and procedures that have been developed to safeguard Monroe County Community College's confidential data in accordance with both state and federal regulatory laws and requirements that have been established to protect information.

All associated persons employed by Monroe County Community College, hereafter referred to as MCCC, are required to understand and abide by these policies.

II. Data Classification

All data that comes into the custody of an MCCC employee during the course of their professional duties is to be classified into one of three categories: Public, Limited, or Restricted. Each classification is to be given a unique set of guidelines on how, when, and with whom to be shared. All employees are to be familiar with all guidelines and responsibilities associated with each classification.

Any questions regarding classifications or usage of data can be directed to Director of Institutional Effectiveness and Chief Data Officer or designee.

All information deemed limited or restricted is to only be accessible to those employees that have a legitimate business reason for viewing. Any knowledge obtained while accessing limited or restricted information is to be used for college business purposes only. All third-party entities with access to MCCC data are required to be contractually bound through either a non-disclosure agreement or specific language in the agreed upon business contract that details handling of limited or restricted data before being allowed access. Any new data that has not been formally classified is considered limited unless otherwise stated by the responsible MCCC employee. The classification of data, as well as access to and use of data, are subject to review and action by the Data Governance Board.

III. Restricted Information

Restricted Information is defined as any information that, if divulged in a non-approved fashion, may lead to civil or criminal liability.

Any and all access to restricted information is to be limited to authorized college personnel and approved third party entities. All electronic access and/or storage must conform to the approved MCCC procedures. In addition, restricted information that needs to be shared to approved outside vendors must be encrypted and/or password protected before being transmitted via secure methods that have

been approved by the Vice President of Finance & Administration or designee.

Examples of Restricted Information

- Social Security Numbers
- Credit Cardholder Information
- Checking or Savings or other Bank Account Number(s)
- Debit Card Numbers
- Password(s)
- Disability Information
- Health and Medical Information
- Library Circulation Records

IV. Limited Information

Limited information is defined as any information that is not public or restricted and can, in conjunction with other pieces of limited and/or restricted information, be used to identify that particular person. As an example, a class list is in itself not useful unless combined with other pieces of information.

Examples of Limited Information

- Staff and student home address and phone number information
- FERPA directory information
- Class lists
- Student Records
- Database access lists
- Payroll information
- Beneficiary/Dependent information
- Benefit elections
- Campus Safety & Security Incident reports
- MCCC Identification numbers
- Drivers' license numbers
- Date of Birth information
- Ethnicity
- Purchasing information designated as proprietary or confidential
- HIPAA protected information

V. Public Information

Public Information is information that is open to the public and that can freely be given to anyone without any damage to the College or to individuals.

There are no limitations on releasing public data but all information regardless of classification will comply with the appropriate data retention policies as well as data destruction policies. If data has a mixture of public and restricted data, by default, the restricted data procedure applies.

Examples of Public Information

- Publicly posted press releases
- Publicly posted schedules of classes
- Published College catalogs
- Information authorized for posting on the College's public website
- Online staff directory, interactive maps, newsletters, etc.
- High-level aggregate enrollment data
- Board of Trustees agenda and minutes

VI. Training

Full training and explanations of the policies related to information security will be conducted for all employees and subsequent trainings shall be given on an ongoing basis for refresher courses as well as changes in procedure. Training will be given at least on an annual basis.

VII. Physical Security

Access to the IT department's work area as well to any closet or room housing IT department equipment is to be controlled via physical locks and limited to authorized personnel only.

All backups on physical media are to be remanded to a secure storage location on campus with access limited to authorized personnel only. A reputable third-party vendor who specializes in offsite backups will be utilized for redundant backups.

VIII. Network Security

All network traffic going to or coming from MCCC controlled assets on either the main campus or the Whitman Center will pass through a firewall that controls access by either firewall rules or Access Control Lists. No remote access to any network resource is possible from outside the network unless multi-factor authentication is used. All network traffic is over a secure medium unless otherwise authorized by the IT department manager.

All electronic mail goes through a spam and antivirus filter to reduce the amount of spam and undesirable/malicious traffic.

IX. Account Security

All new employees are created an account with the minimum privilege level needed. Any subsequent privileges are granted on a case-by-case basis. Administrator accounts are provided as needed with the approval of the IT department. All passwords must meet the MCCC password procedure standard. All employees will be required to use multi-factor authentication for their MCCC accounts as Conditional Access policies permit.

Vendor accounts can be utilized multiple times after creation but should only be enabled when

the vendor specifically requests access and while an MCCC IT employee is monitoring usage.

X. Server Security

All servers will be built on a standard VM template. Servers will be built according to industry standards. Each server will house a separate application and will be kept up to date with patches and updates according to best practices. Remote access will require multi-factor authentication in order to access resources on campus. Physical servers are not utilized unless given permission from the IT manager. Any server, be it physical or virtual, being decommissioned is zeroed out and wiped according to DOD standards. When decommissioning a physical server or virtual host, the platters of the hard drive are physically destroyed.

XI. Desktop Security

All desktops are built on a standard image with the minimum number of applications and services necessary for operation. Remote access will require multi-factor authentication in order to access resources on campus. All user workstations being reused will be zeroed out according to DOD standards and will have the platters of the hard drive physically destroyed when being decommissioned. Any desktop computer that is not able to be managed by MCCC management systems will be segmented from the rest of the MCCC network.

XII. Incident Response

Any MCCC employee with a confirmed or suspected security breach must contact the IT Department. Once an incident has been declared, the incident response team will meet. The incident response team will consist of any relevant members of the IT department and financial department as well as the respective managers. Once the incident response team is formed, the incident response procedure will be activated as well as any third-party vendors on retainer for such an occasion.

XIII. Additional Policies

Please see the MCCC website for additional related policies and procedures such as our HIPAA privacy policy, acceptable use policy, FERPA policy, red flag policy, etc.