INFORMATION CLASSIFICATION

All MCC Employees are required to protect and maintain information at MCC. Until the data has been properly classified, it must be handled as though it is Confidential and appropriate protections must be applied.

PURPOSE

The purpose for this procedure is to identify the criteria for classifying MCC information.

APPLICABILITY

All employees, students, contractors, third party providers and visitors of MCC. This procedure applies to all information at MCC.

CONFIDENTIAL INFORMATION

Confidential Information classification criteria:

1. Requires protections to the highest possible degree as is prudent or required by law to include the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach Bliley Act (GLBA).
2. Loss, improper use or disclosure will likely cause significant harm to an individual, group or MCC.
3. Access is restricted to only individuals who require that information to perform their college functions.
4. Must not be disclosed to parties without explicit management authorization.
5. Must be stored only in an area with sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
6. When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
7. Must not be posted on any public website.
8. Must be securely destroyed when no longer needed.
9. Must be encrypted during electronic transfer.

Examples of Confidential Information include: social security number, grades, financial aid, parent's financial status, accounts receivable transactions, demographic information, personal notes about students, student password, biography, medical, academic history, salaries and benefits, disabilities, evaluations, appointments

SENSITIVE INFORMATION

Sensitive Information classification criteria:

1. Unauthorized disclosure, alteration or destruction could result in a moderate level of risk to the college or its affiliates or involve issues of personal privacy.
2. By default, all data that is not explicitly classified as public or confidential should be treated as Sensitive data.

3. Might be available campus-wide but not available to outside parties or the public.
4. A reasonable level of security controls should be applied to Sensitive data, such as:
    a. Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
    b. Must be stored in an area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
    c. Must not be posted on any public website.
    d. Must be securely destroyed when no longer needed.

Examples of Sensitive Information include email address, major field, dates of attendance, degree, honors and awards received, employment, home/mobile phone number, home email address.

PUBLIC INFORMATION

Public Information classification criteria:

1. Available or distributed to the general public regularly or by special request.
2. Unauthorized disclosure, alteration or destruction would result in little or no risk to the college and its affiliates.
3. Limited controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of such data

Examples of public information include press releases, annual reports, course information, and publicly accessible web pages.

ADDITIONAL PROTECTIONS

All devices containing the above information must be protected at the same level as the data that is stored on them. This include phones, iPads, laptops, notebooks, workstations, etc and personal devices that have MCC information.