

**MAINE COMMUNITY COLLEGE SYSTEM**

**INFORMATION TECHNOLOGY  
Section 903**

**SUBJECT: INFORMATION CLASSIFICATION**

**PURPOSE: To create uniform standards for classifying M CCS information and data**

To ensure that M CCS information and data is properly protected in compliance with applicable federal and state laws, M CCS shall create and implement standards for the classification of information. All M CCS information and any other information stored on M CCS equipment will be classified using the Information Classifications Table set forth in the Appendix hereto.

Information classification will be used to ensure that all M CCS information is properly identified and classified, and will be appropriately handled according to its value, legal requirements, sensitivity, and criticality to M CCS. Further, all M CCS information must be classified to ensure that the information receives the appropriate levels of security to safeguard its confidentiality, integrity, and availability, which will assist in the prevention and detection of identity theft. Finally, the classifications for all information will be regularly reviewed and maintained to ensure that the protection of M CCS information is consistent with all applicable laws and regulations, particularly in regards to personally identifiable information and protected health information.

Procedures governing information classification are set forth in Section III of the M CCS Information Technology Procedures Manual and shall include at a minimum:

1. Information Classification Categories;
2. Expectations for Classifying information;
3. Requirements for College and System Office Leadership;
4. Requirements for Information Owners;
5. Requirements for Information Custodians;
6. Requirements for Information Users;
7. External Information Handling Requirements;
8. Requirements for Providing M CCS Information to External Parties;
9. Information Security Incident Reporting; and
10. Non-Compliance and Sanctions.

---

REFERENCES: 15 U.S.C. §§ 6801 and 6805; 16 CFR § 314

DATE ADOPTED: June 13, 2018

**APPENDIX**

**Information Classification Table**

<b>Information Classification</b>	<b>Description</b>	<b>Examples</b>
<b>RESTRICTED</b>	<p>Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as 'non-public personal information' (NPPI) about people or critical business, academic or research operations under the purview of the Information Owner. Restricted data includes, but is not limited to, data that MCCS is required to protect under regulatory or legal requirements. Unauthorized disclosure or access may:</p> <ol style="list-style-type: none"> <li>1. subject MCCS to legal risk,</li> <li>2. adversely affect its reputation,</li> <li>3. jeopardize its mission</li> <li>4. present liabilities to individuals (for example, HIPAA penalties).</li> </ol>	<ul style="list-style-type: none"> <li>• Bank information</li> <li>• Login Credentials (username &amp; password)</li> <li>• Credit/Debit Card Number</li> <li>• Driver’s License Number</li> <li>• Human Resources information if it contains SSNs, medical reports, etc.</li> <li>• Passport Number</li> <li>• Protected Health Care Information (PHI)<sup>1</sup></li> <li>• Protected Data Related to Research<sup>2</sup></li> <li>• Social Security Number</li> <li>• Student Disciplinary, or Judicial Action Information</li> <li>• Police Records</li> <li>• Student Records (FERPA)</li> </ul>
<b>INTERNAL</b>	All other non-public information not included in the Restricted category.	<ul style="list-style-type: none"> <li>• Licensed Software</li> <li>• Other MCCS Owned Non-Public Data</li> <li>• MCCS Identification Number or Information Number (employee numbers, student ID numbers, etc.)</li> </ul>
<b>PUBLIC</b>	All public information.	General access data, such as that on unauthenticated portions of any college or system managed website.

<sup>1</sup>

Protected Health Care Information includes, but is not limited, to the following:

- Protected Health Information (PHI) or Electronic Protected Health Information (EPHI)
- Patient health-care and human subjects research records
- Payment transactions related to health services
- Medical and personal information in research records
- Quality-assurance and peer-review information from patient care units

<sup>2</sup>

Protected Data Related to Research

- MCCS proprietary information, including copyrightable and patentable information
- Proprietary information belonging to other individuals or entities, such as under a non-disclosure agreement or contract
- Library circulation records and any information about use of any library information resource in any format

