MAINE COMMUNITY COLLEGE SYSTEM

INFORMATION TECHNOLOGY
Section 906

SUBJECT: INFORMATION SYSTEMS RISK MANAGEMENT

PURPOSE: To establish a uniform process and standards to ensure secure and sustainable information systems

It is the policy of MCCS to maintain secure and sustainable technology ecosystems that safeguard all information assets while providing necessary and relevant information access to authorized users. In furtherance of this policy, MCCS shall systematically identify potential threats and known vulnerabilities in any MCCS information system architecture, and identify mitigation recommendations. Regularly scheduled security risk analysis consisting of business process evaluation and information technology system scans shall be performed and documented and the security risk analysis shall be updated annually based on the inherent risk. The inherent risk derived from the outcomes of the system security analysis will be ranked and mitigations identified and performed based on the analysis outcomes.

Information systems risk management procedures are set forth in Section VI of the Information Technology Procedures manual and shall include at a minimum:

1. Roles and Responsibilities for Risk Management;
2. Identification of All Critical Resources and Systems;
3. Identification of All Non-Critical Systems;
4. Manual Risk Assessment of Business Processes;
5. Electronic Risk Assessment and Independent Systems Scans (External and Internal);
6. Risk Identification and Mitigation Process (Including Classification Matrix); and
7. Reporting Standards and Procedures for Identified Risks.

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

DATE ADOPTED: June 13, 2018