**MAINE COMMUNITY COLLEGE SYSTEM**

**PROCEDURES MANUAL**

 **INFORMATION TECHNOLOGY**

**Section 902.1**

**Subject: information security**

**PURPOSE: To form an Information Security Advisory Council to monitor, evaluate and update appropriate procedures for the protection of MCCS information and data.**

**1. Introduction – Cybersecurity Safeguards; WISP**

To assist MCCS in the fulfillment of its obligations under state and federal laws and regulations, including but not limited to the Gramm-Leach-Bliley Act, FTC Safeguards Rule, 16 C.F.R. Part 314, which require the development a comprehensive written information security program implement and monitor appropriate cybersecurity safeguards—aka “controls”, MCCS Presidents’ Council has adopted a written information security program (“WISP”) which applies to all employees (faculty, staff, and student employees), officers, contractors, volunteers, and vendors of MCCS, and establishes information security requirements for all records and other information owned, held, maintained, or managed by MCCS that contain personal information in any format and on any media, whether in electronic or paper form. In accordance with its terms, the WISP requires MCCS to : **(i) designate the employee(s) responsible for coordinating the information security program; (ii) identify and assess risks to personal information MCCS collects, creates, uses and maintains; (iii) design and implement an information safeguards program;** (iv)s**elect appropriate service providers that are capable of maintaining appropriate safeguards at all times in accordance with the WISP; and (v) regularly monitor, evaluate, and update the WISP through periodic reviews by the ISAC (defined below).**

**2. Information Security Advisory Council**

MCCS shall at all times maintain an Information Security Advisory Council (“ISAC”) to periodically evaluate and update the WISP. The ISAC shall oversee the implementation and maintenance of the administrative, technical, and physical safeguards MCCS has selected to protect the personal information it collects, creates, uses, and maintains.

The ISAC shall be comprised of individuals appointed by the MCCS System President from time to time and shall include the following minimum standing members:

* + 1. General Counsel
		2. Chief Financial Officer
		3. Chief Information Officer
		4. Chief Information Security Officer
		5. Presidents of two Colleges

The ISAC shall have the following responsibilities:

1. Recommend for approval by the Presidents’ Council such modifications and amendments to the WISP that may be appropriate from time to time in order to fulfil the intent of the WISP and to comply with applicable federal and state laws and regulations and related guidance;
2. Ensure proper and sufficient resources are available to administer the WISP;
3. Ensure that the controls and requirements of the WISP are properly coordinated with the System Office and Colleges;
4. Ensure the timely completion of training requirements required under the WISP; and
5. Review all information security assessments and audits and ensure that proper and timely response measures are enacted.

The ISAC shall:

1. Be chaired by the Chief Information Security Officer, who shall maintain minutes and action logs following each meeting of ISAC; and
2. Meet not less often than quarterly.

This procedure is adopted in furtherance of MCCS Policy 902 to assist MCCS in fulfilling its responsibilities to safeguard and maintain the security of its information and data and to comply with applicable state and federal laws and regulations, including the Gramm-Leach–Bliley Act.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

DATE ADOPTED: March 26, 2024

DATE(S) AMENDED: