MAINE COMMUNITY COLLEGE SYSTEM

INFORMATION TECHNOLOGY
Section 905

SUBJECT: SECURITY BREACH MANAGEMENT AND NOTIFICATION

PURPOSE: To establish a uniform security breach management and notification process and guidelines for compliance with breach notification requirements

MCCS collects non-public personal information, such as social security numbers and credit card information, as allowed by law and MCCS policy, and as required for MCCS business purposes. Such information is classified as Restricted pursuant to MCCS Policy 903. It is the policy of MCCS to protect Restricted information that it receives, handles, and stores and to comply with laws pertaining to the safeguarding of Restricted information, including laws governing security breaches.

It is essential that members of the MCCS community are both knowledgeable and vigilant about requirements for collecting, retaining and controlling access to Restricted information; identifying potential security breaches; and reporting all security breaches to MCCS personnel for immediate evaluation and action. MCCS shall thoroughly and expeditiously investigate all reported security breaches and take the requisite steps to address the cause of any breach. In those situations when notification of potential victims of a security breach is required by law or otherwise appropriate, MCCS shall do so as expediently as possible, without unreasonable delay and consistent with the requirements of MCCS Procedure 203.1 (Notice of Risk to Personal Data).

REFERENCES: 10 M.R.S.A. §§1346-50-A; *MCCS Policy 903; MCCS Procedure 203.1*

DATE ADOPTED: June 13, 2018
DATE(S) AMENDED: June 23, 2021