MAINE COMMUNITY COLLEGE SYSTEM

INFORMATION TECHNOLOGY
Section 904

SUBJECT: RED FLAG RULE AND IDENTITY THEFT

PURPOSE: To establish a policy to prevent, detect and mitigate identity theft

MCCS recognizes that some of its financial transactions are subject to the provisions of the federal Fair and Accurate Credit Transactions Act of 2003 and the Federal Trade Commission's Red Flag Rule. These laws require MCCS to provide information to assist individuals in the prevention, detection, and mitigation of identity theft from certain data stored or processed by MCCS. MCCS also recognizes its responsibility to minimize the risk of identity theft, regardless of the transaction or area of operation from which it may originate.

To meet its federal compliance obligations and to protect against the personal difficulties that can arise when an identity is stolen, MCCS shall implement and maintain an Identity Theft Compliance Program ("Program"). The Program shall include procedures for the detection, prevention and mitigation of identity theft in its covered accounts and provide guidance to employees to identify inconsistencies, or "Red Flags," in specific financial transactions that warrant further investigation when detected.

The Program is set forth in Section IV of the Information Technology Procedures Manual and shall include at a minimum:

1. Covered Transactions;
2. Relevant Red Flags;
3. Detecting the Presence of a Red Flag;
4. Responding to Detected Red Flags;
5. Outside Vendors;
6. Prevention and Detection of Identity Theft in Other Operations;
7. Policy Administration and Updates.

MCCS requires employees whose duties require access to covered accounts to be familiar with the provisions of the Program to ensure that timely and effective measures are taken to prevent, detect and report identity theft from MCCS information.

REFERENCES: 15 U.S.C. § 1681s(a)(1); 16 CFR § 681

DATE ADOPTED: June 13 , 2018