MAINE COMMUNITY COLLEGE SYSTEM
PROCEDURES MANUAL

GENERAL ADMINISTRATION
Section 203.1

SUBJECT: NOTICE OF RISK TO PERSONAL DATA

PURPOSE: To establish a procedure to provide notice of risk to personal data

I. Introduction

This Procedure complies with the provisions of the Notice of Risk to Personal Data Act.

II. Definitions

As used in this Procedure, the following terms have the following meanings:

A. Breach of System Security

"Breach of system security" means an:

1. Unauthorized acquisition of College or System computerized data that compromises the security, confidentiality or integrity of an individual's personal information maintained on a College or MCCS computer; and/or

2. Authorized acquisition that is then used for an unauthorized disclosure of such personal information.

B. Personal Information

"Personal information" means the following information about an individual when such information is not encrypted or redacted:

1. First name or first initial; and

2. Last name; and

3. Any one or more of the following:
   a. Social security number;

   b. Driver's license number or state identification card number;

c. Account number, credit card number or debit card number, if such a number could be used without additional identifying information, access codes or passwords;

d. Account passwords or personal identification numbers or other access codes; or

e. Any of the data elements contained in paragraphs a through d above when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

"Personal information" does not include information available to the general public from federal, state or local government records, widely distributed media, or other lawful source.

C. Unauthorized Person

"Unauthorized person" means a person who:

1. Does not have authority or permission to access such personal information; and/or

2. Obtains access to such personal information by fraud, misrepresentation or similar deceptive practice.

D. Information Broker

“Information broker” means any person who, on behalf of a College or the MCCS, maintains computerized data that includes personal information.

III. Duty to Investigate

If an information broker becomes aware of a breach of system security, the information broker shall promptly contact the College and/or MCCS Director of Information Technology. Such Director shall then promptly inform the College President and commence a reasonable and good faith investigation to determine the likelihood that personal information has been or will be misused.

IV. Duty to Notify

If a College and/or MCCS Director of Information Technology determines that it is likely that personal information has been or will be misused as result of a breach, the College or MCCS Director of Information Technology shall provide the following notice.

A. Content of Notice

The notice shall contain the date of the breach; the information believed to be accessed; a summary of the college's efforts in response to the breach; and a College or MCCS contact who upon request can provide additional information.

B. Recipients of Notice

The above notice shall be provided to:

1. A person whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person; and

2. The MCCS Director of Information Technology, who in turn shall notify the MCCS President; and

3. The MCCS General Counsel, who in turn shall notify the Maine Attorney General's Office; and

3. In breaches affecting more than 1,000 persons at a single time, the following consumer reporting agencies shall also be notified:

   a. Experian
   P.O. Box 2002
   Allen, TX 75013-2002
   1-888-397-3742

   b. Trans Union
   P.O. Box 1000
   Chester, PA 19022
   1-800-888-4213

   c. Equifax
   P.O. Box 740250
   Atlanta, GA 30374-0250
   1-800-685-1111

   However, the notice to these agencies shall only include the following: date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

C. Timing of Notice

Notice shall be given as expediently as possible once a College and/or MCCS Director of Information Technology determines that it is likely that personal information has been or

will be misused as result of a breach. However, such timing shall be determined consistent with any:

1. Known legitimate needs of law enforcement; and

2. Measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

D. Means of Notice

Notice shall be by U.S. Mail to last known address. If, however, the cost of providing such notice would exceed $5,000, or if the number of persons to receive notice exceeds 1,000, or if the College and System does not have such an address, the following notice may be given instead:

1. E-mail notice to those whose email addresses are known; and

2. Conspicuous posting of the notice on the College's or System's publicly accessible website; and

3. Notification to major statewide media.

V. Complete Copy of the Law

For a complete copy of the Maine law governing this subject, see *10 MRSA §§1346-50-A* available at http://janus.state.me.us/legis/statutes/10/title10ch210-B.rtf.

REFERENCES: 10 M.R.S.A. §§1346-50-A

DATE ADOPTED: January 24, 2007

DATE(S) AMENDED: January 26, 2010