COUNTY COLLEGE OF MORRIS

Personal Information Security Breach Notification Procedure

This procedure has been established in support of the County College of Morris Board of Trustees Identity Theft Protection Program Policy (Trustee Policy 2.2014).

The College's Personal Information Security Breach Notification Procedure governs how the College will respond to incidents involving breach of personal information.

Definitions

"Breach of Security" means an incident of unauthorized access to and acquisition of records containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the College for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business of the College or subject to further unauthorized disclosure.

"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. Records do not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.

"Individual" means a natural person.

"Personal Information" is defined to mean an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.

"Evaluation Oversight Team" comprised of the Vice President for Business & Finance and the Vice President of Institutional Effectiveness / Chief Information Officer, is responsible for oversight, investigation and evaluation of reported breaches of personal information security.

"Program Administrator" assigned to the Director of Budget & Compliance is responsible for coordination of responses to identity theft as delegated by the Evaluation Oversight Team. In addition, the Program Administrator is responsible for compiling and maintaining all documentation of reported breaches of personal information security.

Procedures in the Event of a Security Breach

Internal Reporting

Anyone with knowledge of a security breach of personal information at the County College of Morris shall take the following actions:

i. The first priority after any type of breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible (including the President's cabinet member who oversees the office where the breach is discovered). The records must be secured, and the reasonable integrity, security, and confidentiality of the records or records systems must be restored.

ii. Notify any member of the Evaluation Oversight Team and/or the Program Administrator.

iii. The manager/director of the office for which the discovery was made shall complete the Identity Theft Detection / Breach of Personal Information form, which shall be submitted to the Program Administrator for review by the Evaluation Oversight Team. This form will document the breach, the scope of the breach, steps taken to contain the breach, and names of individuals whose information was, or may have been accessed or acquired by an unauthorized person.

iv. The Evaluation Oversight Team shall inform the President of the incident, conduct an investigation concerning the incident and verify all actions necessary to contain the breach have been implemented.

Notification to Victims where there has been a Security Breach.

Where there has been a security breach the Evaluation Oversight Team will coordinate the notification as outlined below:

i. In advance of the disclosure to the victims of the security breach, the College will report the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to appropriate law enforcement entities.

ii. The college shall notify affected individuals without unreasonable delay; however this notification shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that the agency has made a request that the notification be delayed.

iii. The responsibility for providing notification to affected individuals shall lie with the Program Administrator.

iv. The College Attorney may assist in drafting the notification or review the notification before it is sent.

v. Copy of the notification will be provided to the Director of Marketing and Public Relations prior to the time it is sent to affected individuals.

Contents of the Notification.

The notification shall be clear and conspicuous and include the following:

i. A description of the incident in general terms;

ii. A description of the type of personal information that was subject to the unauthorized access or acquisition;

iii. A general description of the actions taken by the College to protect the personal information from further unauthorized access;

iv. A telephone number that the individual may call for further information and assistance;

v. Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;

vi. The toll-free numbers and addresses for the major consumer reporting agencies.

vii. The federal Trade Commission's website and its toll free number.

Method of Notification:

Notification to affected individuals must be provided by one of the following methods unless substitute notification is permitted;

i. Written notification, or

ii. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001).

Substitute notification: If the cost of providing notice will exceed $250,000, or the total number of individuals to be notified exceeds 500,000, or the College does not have sufficient contact information, substitute notification shall consist of;

i. E-mail notice when the college has a valid email address of the individuals affected;

ii. Conspicuous posting of the notification on the College Internet web site; and

iii. Notification to major Statewide media.

In addition to any disclosure or notification required, in the event that more than 1,000 individuals need to be notified as a result of the security breach, the College shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s.1681a), of the timing, distribution and content of the notification.

News Media Inquiries

All inquiries from the news media should be directed to the Director of Marketing & Public Relations.