
Title: **MILWAUKEE AREA TECHNICAL COLLEGE
PROCEDURE FOR DATA SECURITY BREACH**

Code: HH0101-1

Policy Reference: Wis. Stats. §134.98; H0101-1, Data Services

Milwaukee Area Technical College (MATC) collects and maintains personal data on its students and employees as part of its normal course of business and in compliance with federal and state statutes and regulations. A breach of that data occurs when MATC knows that personal information in its possession has been acquired by a person whom MATC has not authorized to acquire it (a "Data Breach"). "Personal Information" is a person's first name (or first initial) and last name, in conjunction with one or more of the following:

- a. Social security number;
- b. Driver's license number or state identification number;
- c. Financial account number, including credit or debit card account numbers, or any security or access codes or passwords that would allow access to the individual's financial account;
- d. DNA profile; or
- e. Unique biometric data.

Personal Information does not include publicly available information that MATC believes has lawfully been made available to the general public through the media, from federal, state, or local government records, or through disclosures to the general public required by federal, state, or local law.

Procedures to Follow When a Data Breach is Discovered

1. Discovery of Breach. When a Data Breach is discovered, the individual making the discovery shall immediately notify the individual's supervisor. The supervisor shall inform the following who constitute the Data Breach Team:
 - a. The Office of General Counsel;
 - b. The appropriate division head in the area in which the potential breach occurred;
 - c. The Director of Public Safety; and, where applicable,
 - d. The Associate Vice President of Information Technology.
2. Investigation. The Data Breach Team will commence an investigation within 24 hours of the discovery of the Data Breach. The investigation will result in a written report and shall include but not be limited to:

Approving Authority:
Vice President and General Counsel

Date:
6/24/10

Title: **MILWAUKEE AREA TECHNICAL COLLEGE
PROCEDURE FOR DATA SECURITY BREACH**

Code:

Policy Reference: Wis. Stats. §134.98; H0101-1, Data Services

- a. An interview of the person discovering the Data Breach and that individual's supervisor;
 - b. An interview of the caretaker of the information (if different than that in sub. a);
 - c. A determination of the content and scope of information breached; and
 - d. A determination, where possible, of who committed the breach.
3. Material Risk of Identity Theft or Fraud. After all evidence is collected but not longer than 30 days after the discovery of the Data Breach, the Data Breach Team will review the written report and determine whether the Data Breach creates a material risk of identity theft or fraud. If the team concludes there is no material risk of identity theft or fraud, no further action is necessary.
4. Notice. If the Data Breach team concludes there is a material risk of identity theft or fraud, MATC will provide notice to each subject of the breach within 45 days after MATC's discovery of the Data Breach. Notice will be by mail or by the method MATC has previously used to communicate with the subject(s). If, after reasonable attempts, MATC cannot determine the mailing address of the individual, and if MATC has not previously communicated with that individual, MATC will provide notice by a method reasonably intended to provide actual notice to the person.