Series 3000: Operations, Finance, and Property

3100 General Operations

3110 Data Breach Response

"Data breach," as used in this Policy, means "a breach of the security database" as defined in the Michigan Identity Theft Protection Act.

If the District experiences a data breach or receives notice of a breach of a database with District data, the Superintendent or designee, with the assistance of other staff or consultants as necessary, must do the following:

A. Assess and Investigate the Data Breach

1. Make a reasonable effort to identify the cause of the data breach and secure known access points.

2. Promptly conduct a reasonable investigation to determine the extent of the data breach and the identity of persons whose personal information has been compromised. The investigation will include, to the extent possible, an assessment of the software, hardware, and physical documents that were accessed; which personnel and third parties had access to the compromised data; and what specific information was compromised.

3. Contact legal counsel, insurance carriers, and any other person or consultant necessary to investigate the cause of or response to the data breach. If appropriate, the Superintendent or designee may also contact law enforcement.

B. Notifications Involving Michigan Resident Data

1. Promptly notify:

a. each Michigan resident whose personal information was accessed, including encrypted information, if the person accessing the information also had unauthorized access to the encryption key;

b. any other person or organization that owns or licenses data subject to a data breach affecting a Michigan resident; and

c. each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if more than 1,000 Michigan residents receive notice of the breach.

2. Notices must:

a. be in writing;

© 2025 THRUN LAW FIRM, P.C. POLICY SERVICE

b. describe the data breach in general terms, the type of personal information accessed in the data breach, the District's response to protect data from further breaches, and remind the affected person of the need to remain vigilant for incidents of fraud and identity theft;

c. include the District's telephone number and any other telephone number where the recipient may receive additional information; and

d. whenever possible, be mailed to the postal address of the affected person.

C. If a data breach or other digital intrusion compromises information of a non-Michigan resident, comply with the data breach notification law of that resident's state.

Legal authority: MCL 445.63, 445.72

Date adopted: October 26, 2026

Date revised:

© 2025 THRUN LAW FIRM, P.C. POLICY SERVICE