

Office Methods and Data Management

Privacy Protection - Breach of Security

The district will respond to a breach in security immediately and in accordance with law.

Definitions

Breach of Security or Breach B Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information. Good-faith acquisition of personal information by a district employee or agent for a legitimate district purpose is not a breach of security provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

Personal Information B An individual=s first name or first initial and last name in combination with any one (1) or more of the following:

1. Social Security number.
2. Missouri Student Identification System (MOSIS) number, driver=s license number or other unique identification number created or collected by the district or any other government body.
3. Financial account number, credit card number 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.
4. Unique electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual=s financial account.
5. Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional.
6. An individual's health insurance policy number, subscriber identification number or any unique identifier used by a health insurer to identify an individual.

Personal information does not include information that is encrypted, redacted or altered in such a manner that the name or data elements are unreadable or unusable. It also does not include information that is lawfully obtained from publicly available sources or from government records made available to the general public.

Security

All district staff and agents must immediately notify the superintendent or designee if there is a potential breach in the security of personal information. The superintendent or designee will investigate the incident immediately and make a determination as to whether a breach did occur.

If the superintendent or designee, after an appropriate investigation or consultation with the relevant federal, state or local agencies responsible for law enforcement, determines that a risk of identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and will be maintained for five (5) years. If the superintendent or designee determines that a risk of identity theft is reasonably likely, the district will notify, without unreasonable delay, any person whose information may have been accessed.

This notice may be delayed if a law enforcement agency informs the superintendent or designee that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the superintendent or designee documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. Once the law enforcement agency communicates that notice may be provided, the notice will be provided without unreasonable delay.

If the district must provide notice to more than 1,000 individuals, the district will also notify the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. The district will report to these entities the timing, distribution and content of the notice sent to the persons whose information may have been compromised.

Notice

The notice provided to persons whose information was breached shall minimally include a description of:

1. The incident in general terms.
2. The type of personal information that was obtained as a result of the breach of security.
3. A telephone number that affected consumers may call for further information and assistance, if one exists.
4. Contact information for consumer reporting agencies as defined by law.

Tarkio R-I
April 2012

5. Advice that directs affected consumers to remain vigilant by reviewing account statements and monitoring credit reports.
6. Information about how to obtain a free credit report.

The notice may be made in writing or by e-mail if the person has agreed to receive communications from the district electronically in accordance with federal law. Telephone notice may be used if contact is made directly with the affected person.

Substitute notice may be used if the cost of providing notice would exceed \$100,000 or if the district needs to notify more than 150,000 individuals. The district may also use substitute notice for individuals the district is unable to identify or for whom the district does not have sufficient contact information, but the district will use the regular notice for all other affected individuals.

Substitute notice shall include:

1. E-mail notice when the district has an e-mail address.
2. Conspicuous posting of the notice or a link to the notice on the district's website.
3. Notification to major statewide media.

* * * * *

Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.

Legal Refs: ' ' 210.150, .865, 407.1500, RSMo.
Federal Privacy Act of 1974, 5 U.S.C. ' 552a
E Sign Act of 2000, 15 U.S.C. ' 7001
Fair Credit Reporting Act, 15 U.S.C. ' 1681a
Family Educational Rights and Privacy Act, 20 U.S.C. ' 1232g
Individuals with Disabilities Education Act, 20 U.S.C. ' ' 1400 - 1417
29 C.F.R. ' 1630.14