DATA GOVERNANCE AND SECURITY
(Incident and Data Breach Response Plan)

The goal of the district is to eliminate security incidents and avoid any breach of district data. For that reason, all district employees and agents are required to immediately report to the information security officer (ISO) or designee when they know or suspect that a security incident or data breach has occurred. The superintendent, the ISO and their designees are authorized to contact the district's attorney or other necessary resources to quickly and appropriately address a security incident.

Definitions

Data Breach, Breach of Security or Breach A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information. A breach includes, but is not limited to, incidents in which confidential or critical data has potentially been accessed without authorization or stolen; confidential or critical data has been compromised; or a network hack or intrusion has occurred. 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 An individual's first and last name or first initial and last name in combination with any one 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 Incident An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Incident Response

Once notified of an event, the ISO or designee will identify and remedy the weakness that allowed the security incident to occur, repair any damage that has been done, minimize risk associated with the event, and determine who caused the incident. If the incident was intentional or occurred because a user violated district policies, procedures or training, the individual will be referred to the superintendent or designee for discipline and/or other consequences.

Data Breach

The district's primary goal when a data breach occurs is to recover as much data as possible, provide appropriate notifications of the data breach and prevent further disclosure and harm to district students, employees and business operations.

The ISO or designee will investigate the incident immediately and make a determination as to whether a breach did occur. If a breach did occur, the following steps will be taken as quickly as possible:

1. The superintendent and other appropriate administrative staff will be notified immediately. The superintendent or designee will contact the district's legal counsel, law enforcement and the district's insurance carrier when appropriate.

2. The ISO will determine the status of the breach and will take all appropriate measures to prevent additional loss of data and future breaches.

3. If possible, the ISO will preserve any and all evidence of the breach for future investigation, prosecution, insurance claims and other legal action.

4. The ISO will determine the scope of the breach and will work with law enforcement (when appropriate), the superintendent and the district's legal counsel to determine whether district staff, impacted parents/guardians and students, or the public need to be notified and whether additional government agencies need to be involved.

5. Once the district's data has been secured, the ISO, the superintendent and other relevant staff will meet to evaluate the incident, determine the probable causes of the incident and determine what action should be taken to prevent future incidents.

Notice of Breach of Personal Information

Breaches of confidential personal information are particularly problematic, and the district will take additional steps to prevent theft or fraud. The superintendent and the ISO will ensure that victims of security breaches are appropriately notified as required by law.

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 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 years. If the superintendent or designee determines that 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 Content

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

1. A description of the incident in general terms.

2. A description of 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.

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.

Implemented:

Revised: 11/21/2017

East Carter R-II School District, Ellsinore, Missouri