3047
Data Breach Response

I. Preparation

A data breach is an instance in which personal information as defined by state law or personally identifiable information as defined by federal law is released or accessed in an unauthorized manner. The district will implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information handled by the district. In order to ensure compliance with state and federal law; in the event of a breach the following preparatory steps shall be taken.

A. Data Governance

The superintendent, or their designee, will create an annually updated data directory that will include:

1. Computing devices purchased by the district,

2. Software that is installed on district devices,

3. Approved vendors/contractors that have access to personal information or personally identifiable information,

4. Staff members with access to district devices,

5. Staff members with active usernames and passwords for any district software.

B. New Devices and Software

Any new software or device that is used in a district building for district purposes will be submitted to the superintendent or their designee for inclusion in the directory.

II. Incident Response Plan

A. Assessment and Investigation

1. If the District becomes aware of a data breach it will make every reasonable effort to remedy the cause of the breach as soon as possible.

2. The District will contact its cyber or relevant data breach insurance provider in the event of a suspected breach.

3. The District will conduct a good faith, reasonable, and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose.

4. This investigation will include, but not be limited to, an assessment of what software, hardware, and physical documents were accessed; which District personnel had access to the compromised data; and what specific data was compromised.

B. Notification of Effected Individuals

1. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the district shall give notice to the affected Nebraska resident.

2. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

C. Notification of Law Enforcement and Outside Organizations

1. Should notice of the breach be required to any individual, notice of the breach will be simultaneously sent to the Nebraska Attorney General's office.

2. The Superintendent will determine if the Family Policy Compliance Office will be notified of the breach.

3. The Superintendent will determine if the Privacy Technical Assistance Center will be notified of the breach.

Adopted on: _____
Revised on: _____
Reviewed on: _____