S&S Consolidated Independent School District

Identity Theft Policy and Adopting Resolution

RESOLUTION

A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY

WHEREAS, The Fair and Accurate Credit Transaction Act of 2003, an amendment to be Fair Credit Reporting Act, required rules regarding identity theft protection to be promulgated; and

WHEREAS, Those rules became effective May 1, 2009, and require school districts and other governmental entities to implement and identify theft program and policy, and

WHEREAS, The S&S Consolidated Independent School District has determined that the following policy is in the best interest of the District and its employees. NOW, THEREFORE,

BE IT RESOLVED by the S&S CISD Board of Trustees that the following is hereby approved:

IDENTITY THEFT POLICY

SECTION 1: BACKGROUND

The risk to the District, its employees and stakeholders from data loss and identity theft is of significant concern to the District and can be reduced only through the combined efforts of every employee and contractor.

SECTION 2: PURPOSE

The District adopts this sensitive information policy to help protect employees, customers, contractors and the District from damages related to the loss or misuse of sensitive information.

This policy will:

1. **Define sensitive information;**
2. **Describe the physical security of data when it is printed on paper;**
3. **Describe the electronic security of data when stored and distributed; and**
4. **Place the District in compliance with state and federal law regarding identity theft protection.**

This policy enables the District to protect existing employees, contractors, and students, reducing risk from identity fraud, and minimize potential damage to the District from fraudulent activities. The program will help the District:

1. **Identify risks that signify potentially fraudulent activity;**
2. **Detect risks when they occur;**

3. **Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and**
4. **Update the program periodically.**

SECTION 3: SCOPE

This policy and protection program applies to employees, contractors, consultants, temporary workers and students regarding any sensitive data of which the District may have on file.

SECTION 4: POLICY

4.A: Sensitive Information Policy

4.A.1: Definition of Sensitive Information

Sensitive information includes the following items whether stored in electronic or printed format:

4.A.1.a: Credit card information, including any of the following:

1. **Credit card number (in part or whole)**
2. **Credit card expiration date**
3. **Cardholder name**
4. **Cardholder address**

4.A.1.b: Tax identification numbers, including:

1. **Social Security Number**
2. **Business identification number**
3. **Employer identification numbers**

4.A.1.c: Payroll information, including, among other information:

1. **Paychecks**
2. **Pay stubs**
3. **Bank account numbers**
4. **Cafeteria plan check requests and associated paperwork**

4.A.1.d: Medical information for any employees or customer, including but not limited to:

1. **Doctor names and claims**
2. **Insurance claims**
3. **Prescriptions**
4. **any related personal medical information**

4.A.1.e: Other personal information belonging to any employee or contractor, examples of which include:

1. **Date of birth**
2. **Address**
3. **Phone numbers**
4. **Maiden name**
5. **Names**

4.A.1.f: A "covered account" is any account, established record or other common database entry for any employee, a student or a contractor that may exist in the District's payroll, human resources, purchasing, accounts payable, student management or transportation systems.

4.A.1.g: District personnel are encouraged to use common sense and good judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Texas Open Records Act and the District's open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervision.

4.A.2: Hard Copy Distribution

Each employee and contractor performing work for the District will comply with the following:

1. **File cabinets, desk drawers, overhead cabinets and any other storage space containing documents with sensitive information will be locked when not in use.**
2. **Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.**
3. **Desks, workstations, work areas, printers, and fax machines and common shared work areas will be cleared of all documents containing sensitive information when not in use.**
4. **When documents containing sensitive information are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD) approved shredding device.**

4.A.3: Electronic Distribution – Sensitive information regarding an employee, contractor, or student may not be transmitted via e-mails at any time.

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM

5.A: Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions, contains social security numbers or tax identification numbers, bank account numbers or bank routing numbers or other data that might be used to perpetrate an identity theft crime. Every new and existing customer account that meets the following criteria is covered by this program.

1. **Business, personal and household accounts for which there is a reasonably foreseeable risk to identity theft; or**
2. **Business, personal and house hold accounts for which there is a reasonably foreseeable risk to the safety or soundness of the District from identity theft, including financial, operational, compliance, reputation, or litigation risks.**

5.B: Red flags

5.B.1: The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

1. **Alerts, notifications or warnings from a consumer reporting agency;**
2. **A fraud or active duty alert included with a consumer report;**
3. **A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or**
4. **A notice of address discrepancy from a consumer reporting agency as defined in §334.82(b) of the Fairness and Accuracy in Credit Transactions Act.**

5.B.2: Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

1. **A recent and significant increase in the volume of inquiries;**
2. **an unusual number of recently established credit relationships;**
3. **A material change in the use of credit, especially with respect to recently established credit relationships; or**
4. **an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.**

5.C: Suspicious documents

5.C.1: Documents provided for identification that appear to have been altered or forged.
5.C.2: The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
5.C.3: Other information on the identification is not consistent with information provided by the person presenting the identification.
5.C.4: Other information on the identification is not consistent with readily accessible information that is on file with the District, such as a signature card or a recent check.
5.C.5: An application appears to have been altered or forged, or give the appearance of having been destroyed or reassembled.
5.D: Suspicious personal identifying information
5.D.1: Personal identifying information provided is inconsistent when compared against external information sources used by the District. For example:

1. The address does not match any address in consumer report or in the District database;

2. The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or

3. Personal identifying information provided by the individual is not consistent with other personal identifying information.

5.D.2: Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the District. For example, the address on an application is the same as the address provided on a fraudulent application.

5.D.3: Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the District. For example:

1. **The address on an application is fictitious, a mail drop, or a prison; or**
2. **The phone number is invalid or is associated with a pager or answering service.**

5.D.4: The SSN provided is the same as that submitted by other persons applying to or already employed by the District.

5.D.5: The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other employees or applicants or other persona applying to work for or otherwise do business with the District.

5.D.6: The applicant fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

5.D.7: Personal identifying information provided is not consistent with personal identifying information that is on file with the District.

5.E: Unusual use of, or suspicious activity related to an employee or contractor.

5.E.1: Shortly following the notice of a chance of address for an employee or contractor, the District receives a request for new, additional, or replacement payments, or for the addition of authorized users on the account.

5.E.2: A vendor account that has been inactive for a reasonably lengthy period of time is used.

5.E.3: Mail sent to an employee or vendor is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.

5.E.4: The District is notified that an employee or vendor is not receiving paperwork or checks mailed to them.

5.E.5: The District is notified of unauthorized charges or transactions in connection with a vendor's covered account.

5.E.6: The District receives notice from employees or vendors, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the District.

5.E.7: The District is notified by an employee or vendor, a victim of identity theft, a law enforcement authority, or any other person that has opened a fraudulent account for person engaged in identity theft.

SECTION 6: RESPONDING TO RED FLAGS

6.A: Once potentially fraudulent activity is detected, the District must act quickly as a rapid appropriate response can protect employees, vendors and the District from damages and loss.

6.A.1: Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

6.A.2: The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.A.3: The designated authority may be the Business Manager, the Superintendent, or one of the Assistant Superintendent's.

6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. **Canceling the transaction ;**
2. **Notifying and cooperating with appropriate law enforcement;**
3. **Determining the dollar extent of the possible fraud; and**
4. **Notifying the actual employee(s) or vendor(s) that fraud has been attempted.**

SECTION 7: PERIODIC UPDATES TO THE PROGRAM

7.A: At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

7.B: Periodic reviews will include an assessment of which accounts are covered by the program.

7.C: As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

7.D: Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the District and its covered accounts.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Involvement of management

1. **The Identity Theft Prevention Program shall be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.**

2. **The Identity Theft Prevention Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.**
3. **Operational responsibility of the program is delegated to office of the Business Manager.**

8.B: Staff training

1. **Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with covered accounts or personally identifiable information that may constitute a risk to the District or its covered accounts.**
2. **Appropriate employees must receive initial training in all elements of this program within three (3) months of assuming a position with the District, and annual updated training may be performed or prescribed as needed each year as prescribe by the person designated in Section 8.A.2 above.**

8.C: Oversight of service provider arrangements

1. **It is the responsibility of the District to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.**
2. **A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.**
3. **Any specific requirements should be specifically addressed in the appropriate contract arrangement with an independent service provider.**

8.D: This identity theft program will be incorporated into the Business Office Procedures Manual as an integral part of the District's business operations and safeguards against, fraud, identity theft or other abuse or employees, student or vendor information.

This resolution will take effect immediately upon its passage.

Approved this _____ day of _____, 2010.

_____

Board President,

_____

Board Secretary,