Minnesota Government Data Practices Act - Policy & Procedures for Requesting Information from SWT (“SWT”)

Policy Statement

SWT will provide convenient and timely access to public information in accordance with the Minnesota Government Data Practices Act ("MGDPA"), Chapter 13 of the Minnesota Statutes. The Vice President of Market Solutions is the Responsible Authority ("RA") under the MGDPA and is responsible for managing and fulfilling requests for information under the MGDPA. The Senior Associate General Counsel is the Data Practices Compliance Official" ("DPCO") under the MGDPA and is responsible to respond to questions or concerns regarding data access or other problems. The Manager of IT Management is a "Designee" under the MGDPA appointed by the RA to be in charge of systems containing government data and to receive and comply with data requests under the MGDPA. Whenever possible, SWT will direct requestors to existing sources of public information.

How to Request Public Data

You can ask to look at (inspect) data at our offices, or ask for copies of public data that we keep. You have the right to look at (inspect), free of charge, all public data that we keep. You also have the right to get copies of public data. The MGDPA allows us to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

Charges for copies of data will comply with the MGDPA. The DPCO will respond to the requestor with an estimate of the charges for the copies. Charges must be paid in full prior to the receipt of the copies.

For 100 or fewer paper copies – 25 cents per page

100 or fewer pages of black and white, letter or legal size paper copies cost 25¢ for a one-sided copy, or 50¢ for a two-sided copy.

Most other types of copies – actual cost

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically sending the data.

In determining the actual cost of making copies, we include employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that we cannot copy ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

If, based on your request, we find it necessary for a higher-paid employee to search for and retrieve the data, we will calculate search and retrieval charges at the higher salary/wage.

Data Request Form

All data requests must be in writing. SWT uses the Data Request Form available at http://www.sourcewelltech.org/data-policy. If you do not use the Data Request Form, your request should:

- State that you are making a request for public data under the MGDPA (Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13).
- Include whether you would like to inspect the data, have copies of the data, or both.
- Provide a clear description of the data you would like to inspect or have copied.

You are not required to identify yourself or explain the reason for your data request. However, you may need to provide us with some personal information for practical reasons (for example: if you want us to mail copies to you, you need to provide us with an address or P.O Box). If we do not understand your request and have no way to contact you, we cannot respond to your request.

Data Practices Contacts

Data Request Forms or other written requests must be directed to the following SWT contacts, current as of the version date specified in the footer and which may be updated in the course of business:

Responsible Authority

Bob Seward, Vice President of Market Solutions

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6036

Email: bob.seward@sourcewelltech.org

Data Practices Compliance Official

Susan Mussell, Senior Associate General Counsel

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6216

Email: susan.mussell@sourcewelltech.org

Data Practices Designee

Clint Andera, Manager of IT Management

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6235

Email: clint.andera@sourcewelltech.org

How We Will Respond to Your Data Request

We will acknowledge receipt of your data request within three (3) business days of receipt.

- We may ask you to clarify what data you are requesting.
- We will work with you on a time frame for response, and help narrow the request as much as possible in order to provide the information requested as soon as possible.
- Requestors should understand that requested data may need to be gathered from several departments or individuals.
- If we have the data, but we are not allowed to give it to you, we will tell you as soon as reasonably possible and identify the law that prevents us from providing the data.
- If we have the data, and the data are public, we will respond to your request appropriately and promptly, within a reasonable amount of time by doing one of the following:
    - Arrange a date, time, and place for you to inspect the data at our offices; or
    - You may choose to pick up your copies, or we will mail or email them to you. We will provide electronic copies (such as email or CD-ROM) upon request if we keep the data in that format and we can reasonably make a copy.
    - Response time will be impacted by the size and/or complexity of your request, and also by the number of requests you make in a given period of time.
- Following our response, if you do not make arrangements within twenty (20) working days to inspect the data or pay for the copies, we will conclude that you no longer want the data and will consider your request closed.

The MGDPA does not require SWT to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. For example, if the data you request are on paper only, we are not required to create electronic documents to respond to your request. If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

We are also not required to respond to questions that are not about your data requests, or requests for government data.

Requests for Summary Data

Summary data means reports or statistical data derived from private data and from which all identifying information is removed. If you request summary data, you are required to pay SWT for the costs of preparing summary data, which may include employee time, material programming costs, etc. Within ten (10) business days of receipt of your request, SWT will inform you: (1) whether it is possible to produce summary data without compromising confidentiality, and (2) if so, the time schedule and the estimated

costs for producing the summary data. Charges must be paid in full prior to the information being processed. You may use the Data Request Form to request summary data.

Standing Requests

Standing requests will be honored for sixty (60) days, after which you must renew them to ensure that you are still interested in receiving the data.

Keeping Data Secure

SWT has policies and procedure relating to the privacy and security of information. These policies can be found at: http://www.sourcewelltech.org/data-policy and http://www.sourcewelltech.org/privacy-policy.

In the event of an unfortunate "security incident" or "privacy incident" as defined in such policies, SWT will report the event to its school customers within five (5) business days , subject to any restrictions imposed by law enforcement authorities as described in further detail in the policy.

Data Request Form

Request date:

By completing this form, I am making an official request for data under the Minnesota Government Data Practices Act ("MGDPA"), Chapter 13 of the Minnesota Statutes.

Requestor:

☐ I am a **member of the public** seeking information that is classified as public and is not about me.

- Does not require proof of identity

☐ I am the **data subject**. I am requesting information about myself or that identifies me.

- Requires proof of identity. (See Identity Verification Guide available at http://www.sourcewelltech.org/data-policy for qualifying documents)

☐ I am the **parent or legal guardian of a minor child** seeking information about my child/student.

- Requires proof of identity. (See Identity Verification Guide available at http://www.sourcewelltech.org/data-policy for qualifying documents)

☐ I am the **legal guardian of an individual adult** seeking information about the individual.

- Requires proof of identity. (See Identity Verification Guide available at http://www.sourcewelltech.org/data-policy for qualifying documents)

I am requesting access to data in the following way:

I understand that depending on the nature of my request and how I would like to receive the data, charges may apply. (See SWT's **MGDPA Policy & Procedure** for details)

☐ Inspection - I would like to set up a time to only look at the data.

☐ Copies - I would like to receive a copy of the data in the following manner as available:

☐ I prefer electronic (.pdf) copies if available

- Email address required

☐ I prefer paper copies

- Mailing address or fax required unless picking up

☐ Both inspection and copies - I would like to look at the data first and then decide if I need a copy.

The data I am requesting (include explanation if you are requesting summary data):

Describe the data you are requesting as specifically as possible.

Options to submit this form:

1. Email this form to the Data Practices Contacts identified in SWT's **MGDPA Policy & Procedure**.

2. Print this form and mail it, or deliver it to the Data Practices Contacts identified in SWT's **MGDPA Policy & Procedure**.

If you are required to identify your identity, you must provide the verification documents along with this form (or other writing) to the Data Practices Contacts.

Contact information (optional)*

Name:

phone number:

email address:

street address:

* You are not obligated to provide any contact information unless you are required to verify your identity (See page 1 under *Requestor*). However, if you want us to mail/email you copies of data, we will need some type of contact information. We also need contact information if we do not understand your request. We will not work on your request until we can clarify it with you.

Identity Verification Guide

The following constitute proof of identity.

An **adult individual** must provide a valid photo ID, such as:

- a state driver's license
- a military ID
- a passport
- a Minnesota ID
- a Minnesota tribal ID

A **minor individual** must provide a valid photo ID, such as:

- a state driver's license
- a military ID
- a passport
- a Minnesota ID
- a Minnesota Tribal ID
- a Minnesota school ID

The **parent or guardian of a minor** must provide a valid photo ID *and either:*

- a certified copy of the minor's birth certificate, *or*
- a certified copy of documents that establish the parent or guardian's relationship to the child, such as:
    - a court order relating to divorce, separation, custody, foster care
    - a foster care contract
    - an affidavit of parentage

The **legal guardian for an individual** must provide a valid photo ID *and* a certified copy of appropriate documentation of formal or informal appointment as guardian, such as:

- court order(s)
- valid power of attorney

Note: Individuals whose identity cannot be verified in person must provide a notarized verification using the **Notary Identity Verification Form** available at http://sourcewelltech.org/data-policy.

Notary Identity Verification Form

The following constitute proof of identity. By presenting to a notary, you are attesting that the documents provided are true and correct copies establishing identification and/or relationship to a minor.

An **adult individual** must provide a valid photo ID, such as:

- a state driver's license
- a military ID
- a passport
- a photo ID issued by the state
- a tribal ID

A **minor individual** must provide a valid photo ID, such as:

- a state driver's license
- a military ID
- a passport
- a Minnesota photo ID
- a Minnesota tribal ID
- a Minnesota school ID

The **parent or guardian of a minor** must provide a valid photo ID (see in adult individual section above) ***and*** *either a*

- a certified copy of the minor's birth certificate; *or*
- a certified copy of documents that establish the parent or guardian's relationship to the child, such as:
    - a court order relating to divorce, separation, custody, foster care
    - a foster care contract
    - an affidavit of parentage

The **legal guardian for an individual** must provide a valid photo ID *and* a certified copy of appropriate Documentation of formal or informal appointment as guardian, such as:

- court order(s)
- valid power of attorney

Description of Proof of Identity Documents:

State of Minnesota County of _____

I certify that the documents selected above were presented to me on _____ day of _____,

20_____ and are true and correct copies of such documents in the possession of _____.

Dated: _____

_____

(Signature of Notary Public or other Official)

My Commission Expires: _____

Information on Rights of Subjects of Government Data

Policy Statement

SWT provides educational products and services to school districts and related education entities. In connection with such services, SWT hosts educational data, including student data shared with SWT by its school district customers. SWT also maintains data about its employees and business partners. SWT's adoption of this policy satisfies the requirement set forth in Minn. Stat. §13.025, subd. 3 to prepare a written policy of the rights of data subjects under Minn. Stat. §13.04.

Right to know what data is kept about you and how it is classified

- Upon request, you may be informed about what data is kept about you and whether it is classified as public, private, or confidential. You have the right to see data about yourself that is classified as public, private, or confidential. If SWT maintains data about you that is classified as confidential, you will be told that the information exists, but you will not be able to access the data.

- To access public or private data on yourself, you can make a written request to the Data Request Contacts listed in the following section.

- If you are requesting information on yourself, please be as specific as possible. If you have an employee or student ID number, please include that in your request (if you do not have that information, please include a birthdate or the last 4 digits of your SSN).

- If we do not have the data, we will notify you in writing within ten (10) business days after we receive your request.

- If we have the data, but the data are confidential or private data that are not about you, we will notify you within ten (10) business days receipt of your request and state which specific law says you cannot access the data.

- If we have the data, and the data are public or private about you, we will respond to your request within ten (10) business days after we receive your request by either sending you copies of the information or making arrangements for you to access the data. In some cases, there may be charges for copies of the data we have on you. We will work with you to pay any charges in advance of receiving the data.

- After we have provided you with access to data about you, we do not have to show you the data again for six (6) months unless there is a dispute or we collect or create new data about you.

- The Minnesota Government Data Practices Act ("MGDPA") does not require us to create or collect new data in response to a data request if we do not already have the data, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. In addition, we are not required to respond to questions that are not specific requests for data.

- Private data on you will only be shared with you, with someone who has your written permission, with SWT staff who need the data to do their work, and as permitted by law or court order.

- There is no charge to view data about yourself, but if you are requesting copies of data, there might be a charge for copies. You will be told about any charges in advance.

- Upon request, you will be informed of the content and meaning of the public or private data that is maintained on you.

Data Request Form

All data requests must be in writing. SWT uses the Data Request Form available at http://www.sourcewelltech.org/data-policy. If you do not use the Data Request Form, your request should:

- State that you are making a request for public data under the MGDPA (Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13).

- Include whether you would like to inspect the data, have copies of the data, or both.

- Provide a clear description of the data you would like to inspect or have copied.

You are not required to identify yourself or explain the reason for your data request. However, you may need to provide us with some personal information for practical reasons (for example: if you want us to mail copies to you, you need to provide us with an address or P.O Box). If we do not understand your request and have no way to contact you, we cannot respond to your request.

Data Practices Contacts

Data Request Forms or other written requests must be directed to the following SWT contacts:

Responsible Authority

Bob Seward, Vice President of Market Solutions

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6036

Email: bob.seward@sourcewelltech.org

Data Practices Compliance Official

Susan Mussell, Senior Associate General Counsel

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6216

Email: susan.mussell@sourcewelltech.org

Data Practices Designee

Clint Andera, Manager of IT Management

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6235

Email: clint.andera@sourcewelltech.org

Right to data notice when private or confidential data is collected from you

If you are asked to supply private or confidential data about yourself, you must be told of the intended use of the data, whether you are legally required to provide the data, any known consequences of giving or withholding the data, and which other agencies or persons are authorized by law to receive the data. This notice is commonly known as the Tennessen Warning.

Right to challenge the accuracy or completeness of data about you

- If you think that data maintained by SWT about you is inaccurate or incomplete, you may file a data challenge to try and have the data changed.

- Accurate means that the data are reasonably correct and do not contain factual errors; complete means that the data describe the history of your contact with SWT in a complete way. This procedure is not a substitute for any grievance process available to either data subjects or employees.

- To make a data challenge, write to the Data Contact Resources and state clearly that you are making an accuracy or completeness challenge; identify the data you are challenging, and what you think should be done. You will receive a decision within thirty (30) days whether SWT agrees with your challenge. If we agree, your data will be amended appropriately. If SWT disagrees or believes that your request has to do with something other than the accuracy or completeness of the data, the challenge will be denied.

- If your challenge is denied, you have the right to file an appeal with the Commissioner of the Minnesota Department of Administration. Your appeal must be in writing and filed within sixty (60) days after SWT's decision.

- If you believe that public or private data that SWT maintains about you is inaccurate or incomplete, you have the right to include a statement of disagreement with the data. If the disputed data is released to a third party, SWT will include your statement of disagreement with the data.

Right to have your data protected

- SWT is required under the MGDPA to protect your data. We have established appropriate safeguards to ensure that your data is safe. Our policies can be found at http://www.sourcewelltech.org/data-policy and http://www.sourcewelltech.org/privacy-policy.

- In the event of an unfortunate "security incident" or "privacy incident" as defined in such policies, SWT will ensure that you are notified as required by law.

Data Security Classification Policy

Policy Statement

To protect the security and integrity of SWT data, and comply with the Minnesota Government Data Practices Act ("MGDPA"), Chapter 13 of the Minnesota Statutes, SWT data must be classified appropriately. SWT uses data security classification and security level to ensure all data and the systems on which it is stored, accessed, transmitted, or have the ability to impact the security of the data have appropriate security controls to protect the confidentiality, integrity and availability of the data.

SWT's adoption of this policy satisfies the requirement set forth in Minn.Stat. §13.05, subd. 5 to establish procedures to ensure appropriate access to not public data. SWT limits employees' access to not public data whose work assignment reasonably requires access, or who have a legitimate need to know, and to other entities or individuals authorized by law.

Data Inventory

Under the requirement set forth in Minn.Stat. §13.025, subd. 1, SWT has prepared a Data Inventory available at http://sourcewelltech.org/data-policy which identifies and describes all not public data on individuals and not individuals maintained by SWT. To comply with Minn.Stat. §13.05, subd. 5, the Data Inventory identifies SWT employees who have access to not public data. In the event of a temporary duty assignment by a manager or supervisor, an employee may access not public data for as long as the work is assigned to the employee.

In addition to the employees listed in the Data Inventory, the following employees have access to not public data as necessary for their duties: Managing Director, Vice President Marketing Solutions, Vice President Client Solutions, Vice President Business Development, Manager of IT Management, Senior Associate General Counsel, Human Resources Business Partner, Responsible Authority, Data Practices Compliance Official, and Designee.

Employee position descriptions

Position descriptions may include provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access.

Data sharing with authorized entities or individuals

State or federal law may authorize the sharing of not public data in specific circumstances. Not public data may be shared with another entity if state or federal law allows or mandates it. Individuals will be provided with Tennessen warnings as required under Minn.Stat. §13.04, subd. 2 in accordance with the nature of any data request. Any sharing of not public data will be strictly limited to the data necessary or required to comply with applicable law.

Ensuring that Not Public data is not accessed

SWT ensures that not public data is accessed only by employees as necessary for their job responsibilities by following the procedures set forth in the separate **Data Classification & Control Policy** adopted on August 26, 2009.

Penalties for unlawfully accessing Not Public data

SWT will utilize the penalties for unlawful access to not public data as set forth in Minn.Stat. §13.09 if necessary. Penalties include suspension, termination and/or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Data Classification

SWT data security classifications are:

Confidential (individuals) or Protected Nonpublic (not on individuals) - This classification includes data that is not public and is not accessible to the data subject. It is available to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and other entities or individuals authorized by law.

Private (individuals) or Nonpublic (not on individuals) - This classification includes data that is not public and is accessible to the data subject, and to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and other entities or individuals authorized by law.

Public - This classification includes data that is accessible by anyone for any reason.

Questions

Questions regarding this policy should be directed to either the:

Responsible Authority

Bob Seward, Vice President of Market Solutions

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6036

Email: bob.seward@sourcewelltech.org

-- or to the:

Data Practices Compliance Official

Susan Mussell, Senior Associate General Counsel

2340 Energy Park Dr., Suite 200

St. Paul, MN 55108

Direct: 651-999-6216

Email: susan.mussell@sourcewelltech.org

Data Inventory

This page is intentionally left blank. SWT's **Data Inventory** dated 2014 (when SWT was operating as Technology and Information Educational Services (TIES)) is attached as Pages 1 through 11 of the "*TIES Data Inventory*" for the following categories of data:

- Administration
- Building
- Finance
- Health and Safety
- Payroll
- Personnnel
- Transportation

Breach Notification Policy

Policy Statement

The purpose of this Breach Notification Policy is to provide guidance to the SWT staff in the event of a potential data breach of the SWT system. Generally speaking, under Minnesota law, Minn. Stat. §13.055, subd. 1 (a), a data breach occurs when an unauthorized data access is made with the intent to use the data for a nongovernment purpose. If it is determined that a breach has occurred, the next step is to decide if and when notification is an appropriate response under Minn. Stat. §13.055, subd. 2 (a) and if so, to whom notification must be sent and the information that must be included.

In addition, as a state agency, SWT is subject to the provisions in Minn. Stat. §3.971, subd. 9, that requires notification to the Office of the Legislative Auditor (OLA) if government data "classified by Chapter 13 as *not public*" (Emphasis added) may have been improperly accessed or used. Under this law, SWT may be obligated to notify the OLA even if notification under Minn. Stat. §13.055 is not required.

NOTE: Because SWT is a Minnesota joint powers entity organized under Minn. Stat. §471.59, and the majority of its business is conducted in the state of Minnesota with Minnesota school districts and similar customers, the information in this Policy is based solely on applicable Minnesota law. However, SWT also provides software and related technology services to customers located outside of Minnesota. In the event of a data breach (or potential breach) in another state, SWT may be obligated to respond in a manner that complies with local laws. State security breach laws vary, for example, in the definitions of what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and, exemptions (e.g., for encrypted data, unintentional acquisition or inadvertent internal disclosure). Accordingly, the Breach Notification Team will engage local experts or consultants, e.g., legal counsel, as necessary to understand and comply with local applicable data breach laws.

Keywords

Data breach or breach. As used in this Policy, a data breach or breach is a "Breach of the security of the data" as defined in Minn. Stat. §13.055, subd. 1 (a): an "*unauthorized acquisition* of data maintained by a government entity that compromises the security and classification of the data. Good faith acquisition of or access to *government data* by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the *government data* is not provided to or viewable by an *unauthorized person*." (Emphasis added).

Unauthorized acquistion. This is when a person has obtained, accessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or without statutory

authority - and with the intent to use the data for nongovernmental purposes. Minn. Stat. §13.055, subd. 1 (c).

Unauthorized person. This is any person who accesses government data without a work assignment that reasonably requires access to the data. Minn. Stat. §13.055, subd. 1 (d).

Government data. This means all data collected, created, received, maintained or disseminated by any government entity (e.g., SWT) regardless of its physical form, storage media or conditions of use. Minn. Stat. §13.02, subd. 7.

Private data. This is data on individuals that is not public and is accessible to the data subject. Private data is available to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and to other entities or individuals authorized by law. Minn. Stat. §13.02, subd. 12.

Confidential data. This is data on individuals that is not public and *is not* accessible to the data subject. Confidential data is available to SWT employees with a legitimate need to know, or whose work assignments reasonably require access, and to other entities or individuals authorized by law. Minn. Stat. §13.02, subd. 3.

Not public data. For purposes of this Policy, not public data includes private and confidential data as defined above, and government data classified as private or confidential on a temporary basis. Minn. Stat. §13.02, subd. 8 (a).

Person. This means any individual, partnership, corporation, association, business trust, or legal representative of an organization. Minn. Stat. §13.02, subd. 10.

Breach Notification Team

SWT has established a Breach Notification Team (the "Team") which consists of the following employees:

- Managing Director
- Vice President Marketing Solutions
- Vice President Client Solutions
- Senior Associate General Counsel
- Human Resources Business Partner
- Marketing and Public Relations Manager

All SWT employees have an obligation to report a potential breach to one or more members of the Team. Upon notification of a potential incident, the Team will promptly begin an investigation of the incident consistent with this Breach Notification Policy, and similar policies. The Team will promptly

select an incident lead who will coordinate the investigation as follows (the incident lead may vary depending on each case):

- Assign key tasks to each Team member.
- Manage and coordinate SWT overall investigation and response efforts.
- Act as the intermediary between the Team and SWT Board of Directors.
- Manage timelines and ensure that the investigation and response efforts are documented from beginning to end.
- Engage the resources needed to manage the investigation and breach (e.g., employees, vendors, customers, consultants, outside legal counsel).

Determine Whether a Breach Has Occurred

In general, there has been a breach that triggers notification to ***affected individuals*** under Minn. Stat. §13.055, subd. 2 when all of the following apply:

- A person,
- Views or takes private or confidential data,
- Without permission or statutory authority, and
- With the intent to use the private or confidential data for nongovernmental purposes

NOTE: An important factor to be taken into account by the Breach Notification Team in determining whether there has been a breach is whether or not the private or confidential data is encrypted. If the data is question is encrypted with sufficient complexity and security so that the unauthorized person will be unable to read or understand the data, then a breach of security as defined in Minn. Stat. §13.055, subd. 1 (a) has not occurred. Advisory Opinion 06-030 (Nov. 8, 2006).

In the event of a breach under Minn. Stat. §13.055, individuals whose private or confidential data has been breached must be notified. Details of the required notice are set forth below on page 4.

In general, there has been a breach that triggers notification ***to the OLA*** under Minn. Stat. §3.971, subd. 9 when all of the following apply:

- An entity (e.g., SWT),
- Has knowledge that not public data may have been improperly accessed or used, and
- Regardless of how the unauthorized party intended to use the not public data

The duty to notify the OLA is broader than the duty to notify individuals under Minn. Stat. §13.055. Under Minn. Stat. §3.971, the OLA should be notified if there is a possibility of a breach - and regardless of whether the unauthorized party intended to use the not public data for nongovernmental purposes.

Comparison of Minn. Stat. §13.055 and Minn. Stat. §3.971

Minn. Stat. §13.055	Minn. Stat. §3.971
• When a person with no reasonable, work-related need to access private or confidential data, • Views or takes the data, • With the intent to use the data for purposes unrelated to his/her job, *then* • The subjects of the data must be notified.	• When an entity has knowledge that not public data may have been improperly accessed or used, • Regardless of how the unauthorized party intended to use the not public data, *then* • The OLA must be notified.

Examples of when OLA notification is required, but the notice provision in Minn. Stat. §13.055 is not triggered:

- Accidental access of a not public database by a government employee
- Incorrectly typing an email address and sending not public data to the wrong government employee
- Inadvertently reading a report with not public data without an appropriate work assignment

Each of the above examples require corrective action and notice to the OLA, but does not require notice to affected individuals under Minn. Stat. §13.055 because of the lack of wrongful intent.

How Breaches Often Occur

Common examples of how breaches occur are described below. This list is not intended to be all inclusive:

- Lost or stolen laptops, or removable storage devices (e.g., flashdrives), or smartphones that contain private or confidential data.
- Databases containing private or confidential data are hacked by individuals outside of SWT.
- Employees access private or confidential data without a work assignment.
- Misguided or misaddressed emails or faxes that contain private or confidential data.
- An individual outside of SWT deceives an employee into improperly releasing another individual's private or confidential data.

Requirements of a Breach Notifiation to Individuals Under Minn. Stat. §13.055, subd. 2 (a)

SWT may provide written notice to affected individuals by either first class mail per Minn. Stat. §13.055, subd. 4 (a), or by electronic notice per Minn. Stat. §13.055, subd. 4 (b) (consistent with the provisions

regarding electronic records and signatures set forth in Section 7001, U.S. Code Title 15, Electronic Signatures in Global and National Commerce Act). The notice must comply with the following requirements:

- Be in writing,
- Inform the individual that a report will be prepared about the breach investigation,
- State how the individual may obtain access to the report and that he/she may request a copy of the report by mail or email, and
- Be sent without unreasonable delay (consistent with: (1) the legitimate needs of a law enforcement agency per Minn. Stat. §13.055, subd. 3, and (2) any measures necessary to determine the scope of the breach and to restore the reasonable security of the data).

Substitute notice may be provided if the cost of providing written notice exceeds $250,000, or if the group of individuals to be notified exceeds 500,000, or if SWT does not have sufficient contact information for the individuals. Minn. Stat. §13.055, subd. (c). Substitute notice consists of all the following:

- Email notice if SWT has the email addresses for the affected individuals,
- Conspicuous posting of the notice on SWT website, and
- Notification to major media outlets that reach the general public within SWT jurisdiction. Minn. Stat. §13.055, subd. (c) (i) (ii) and (iii).

Breach Incident Response

There is no single way of responding to a data breach and each breach will need to be dealt with on a case-by-case basis. That being said, the Team should complete following **Ten Steps in the first 24 hours** from learning of a data breach:

1. **Record the date and time** the breach was discovered and when response efforts began.

2. **Contain the breach**. Stop any additional data loss. For example, shut down the system that was breached, revoke computer access privileges, and recover mishandled paper files.

3. **Gather and protect evidence** that may be needed by law enforcement.

4. **Determine the cause and extent** of the breach.

5. **Determine who is or may be impacted** including the states in which any affected individuals reside.

6. **Document everything** known about the breach including who discovered it, who reported it, to whom it was reported, who else knows about it, what type of breach occurred, what data was compromised, what sytems are affected, what devises are missing, was the data encrypted, etc.

7. **Access priorities and risks** based on what is known about the breach.

8. **Review protocols** regarding the notification process.

9. **Advise the Executive Committee** of the breach.

10. **Launch crisis communications process**.

After the checklist in the **Ten Steps in the first 24 hours** is completed, to keep the response plan on track, the following **Next Steps** should be taken:

1. **Fix the issue that caused the breach**: delete any hacker tools, determine if there are other security gaps or risks, replace any affected hardware with clean equipment, implement security precautions as necessary to prevent the same type of breach, document when and how the breach was contained, etc.

2. **Continue working with forensics**: analyze backup, preserved or reconstructed data sources, ascertain the number of likely individuals affected, determine the type of information that was compromised, begin to align compromised data with school districts or other affected customers and individuals - and addresses for notification.

3. **Identify legal obligations**. Review applicable state and federal laws, and contractual obligations that apply to SWT data, determine the people and entities that need to be notified, e.g., individuals, school districts and other customers, state agencies, the OLA, the media, etc., ensure that notifications occur within mandated deadlines.

4. **Reports:** maintain daily breach reports, routinely update the overview of priorities and progress as well as problems and risks that could interfere with the process. For example, other projects and business initiatives may need to be delayed within the organization in order to complete the breach response process.

5. **Communication with the Board of Directors of SWT**: continue regular reports to the Board of Directors as required.

6. **Continue media communications as necessary**.

7. **Consider notifying law enforcement**: conduct that constitutes a knowing unauthorized acquisition of not public data is a misdemeanor and willful violations are subject to criminal penalties and are just cause for suspension without pay or dismissal. Minn. Stat. §13.09. If law enforcement is involved, they may request that SWT wait to notify affected individuals in order to avoid impacting their investigation.

Breach Investigation Report, Minn. Stat. §13.055, subd. 2 (b)

If a breach occurs, SWT is required to complete an report upon completion of the investigation. The report must include the facts and results of the investigation.

If a breach involved unauthorized access to or acquisition of data by an employee, contractor, or agent of SWT, the report must at a minimum include:

- A description of the data that were accessed or acquired, and
- The number of individuals whose data was improperly accessed or acquired.

In addition to the information described above, if there has been a final disposition of disciplinary action against an employee, the report must also include:

- The name of each employee responsible for the unauthorized access or acquisition, and
- The final disposition of any disciplinary action taken against each employee in response.