Breach Notification Policy

Policy Statement

The purpose of this Breach Notification Policy is to provide guidance to Sourcewell Technology staff in the event of a potential data breach of Sourcewell Technology 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, Sourcewell Technology 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, Sourcewell Technology may be obligated to notify the OLA even if notification under Minn. Stat. §13.055 is not required.

NOTE: Because Sourcewell Technology 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, Sourcewell Technology 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, Sourcewell Technology 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., Sourcewell Technology) 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 Sourcewell Technology 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 Sourcewell Technology 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

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

- Chief Operating Officer
- Chief Technology Officer
- Principal Security Architect/Principal Enterprise Architect, CISSP®
- Chief Legal Officer
- Human Resources

All Sourcewell Technology 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, e.g., Sourcewell Technology Data Privacy and Security Policy. 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 Sourcewell Technology overall investigation and response efforts.
- Act as the intermediary between the Team and Sourcewell Technology 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., Sourcewell Technology),
- 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 Sourcewell Technology.
- 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 Sourcewell Technology deceives an employee into improperly releasing another individual's private or confidential data.

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

Sourcewell Technology 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 Sourcewell Technology 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 Sourcewell Technology has the email addresses for the affected individuals,
- Conspicuous posting of the notice on Sourcewell Technology website, and
- Notification to major media outlets that reach the general public within Sourcewell Technology 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 Sourcewell Technology 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 Sourcewell Technology**: 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 Sourcewell Technology 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, Sourcewell Technology 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 Sourcewell Technology, 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.