VERMONT
AGENCY OF EDUCATION

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1130 | (f) 802-828-6430 | education.vermont.gov

School Data Security Breaches and Vermont Law

Purpose

This advisory is intended to provide Vermont supervisory unions and school districts (SU/SDs) with information on the State of Vermont requirements regarding reporting a data breach. The Vermont Agency of Education (AOE) does not govern security breach notifications. As described below, State law has been established to address this process. SU/SDs should consult the law and direct questions on this law to the Vermont Office of the Attorney General.

State of Vermont Guiding Legislation

The Vermont Security Breach Notice Act is the governing law directing how and when a security breach is to be reported. Within that law is set forth the notification requirements for any organization or business to report a security breach. A security breach is defined in 9 V.S.A. § 2430 as the unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of a consumer's personally identifiable information (PII) maintained by the data collector. PII is defined in detail within the law and includes information that schools would be routinely collecting and storing. It is recommended that SU/SDs document the information flow within school operations as part of assessing their current cybersecurity plans. Such a process would include the following:

- Understanding what type of information your SU/SD collects and uses;
- Understanding where the data is located and how it flows within the SU/SD, especially with external partners and vendors;
- Understanding how the SU/SD authenticates users (i.e. passwords, multi-factor techniques) before they are granted access to data; and
- Understanding the training required for users of the data to ensure the security and confidentiality of all PII.

For more on this topic, see the AOE School Cybersecurity advisory, March 2022.

Security Breach Notice Requirements

Specific notification steps for when and how to report a security breach are outlined in 9 V.S.A. § 2435. SU/SD are encouraged to read the law and consult with their legal counsel to ensure a common understanding of what is required in the event a breach occurs. The following are highlights of requirements within the law pertinent to SU/SD.

- Any data collector that owns computerized PII shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the

Contact Information:

If you have questions about this document or would like additional information, please contact:

Lisa Helme, Student Pathways Division at lisa.helme@vermont.gov or (802) 828-6956.

breach. Notice of the security breach shall be made no later than 45 days after the discovery or notification.

- The data collector shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach with 14 business days. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as it is known.
- When the data collector provides notice of the breach to the Attorney General, that notice shall include the number of Vermont consumers affected (if known) and a copy of the notice provided to consumers in accordance with this law.
- The required notice to consumers may be delayed upon request of a law enforcement agency. The data collector shall document such request in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The law enforcement agency shall promptly notify the data collector in writing when the law enforcement agency no longer believes that notification may impede their investigation. The data collector shall then provide notice to the consumer without unreasonable delay upon receipt of the written communication from law enforcement.

Vermont Security Breach Notice Act Guidance from the Attorney General

The Vermont Office of the Attorney General has prepared a security breach guidance document on the law to assist organizations and businesses. Any questions about the guidance should be directed to their office via email at ago.securitybreach@vermont.gov or by calling (802) 828-5479. Within the guidance document is specific direction regarding reporting a security breach.

- Involve law enforcement immediately. Call the FBI or state or local police to report the incident and determine the next steps to take. In Vermont, call the Burlington FBI office at (802) 863-6316. After normal business hours, call the Albany FBI office at (518) 465-7551. Also contact the Vermont State Police Bureau of Criminal Investigation at (802) 244-8781. Section 23 of the security breach guidance document provides more direction.
- Provide confidential preliminary notice to the Attorney General about the breach within 14 days.
- Notify consumers about the breach in the most expedient time possible and not later than 45 days after discovery or notification.
- Notify the three major credit reporting agencies if you are going to send a notice of security breach to more than a thousand consumers.

General Guidance

Within the guidance document provided by the Attorney General is specific information on the content of a consumer notice. There is a bulleted list of information that should be in the notice and a model notice letter in Appendix 2.

In addition to legal requirements for reporting a data security breach, the SU/SD should consider in advance how they will internally address an incident should it occur. AOE has created a Cybersecurity Breach Planning Rubric that can be used as a self-assessment to identify areas of strength as well as those that require additional work. To view the rubric, see AOE Cybersecurity Breach Planning Rubric, March 2022.

Within your SU/SD insurance portfolio may be cyber coverage. It is recommended that SU/SD understand the coverage provided. As part of your cybersecurity planning, document the contact process for notifying the insurance company and incorporate that notification into your data breach response plan.

Resources

Below is a list of organizations and resources on security breach reporting.

Vermont Office of the Attorney General: The office has a publication titled "Vermont Security Breach Notice Act Guidance" on their website. The publication was updated in June 2020. Any questions about the guidance document should be directed to their office via email at ago.securitybreach@vermont.gov or by calling (802) 828-5479.

U.S. Department of Education Privacy Technical Assistance Center: The department regularly updates a frequently asked questions section on its website to allow for easy access to answers to questions on student data privacy and disclosure.

Multi State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. Membership is free to school districts. MS-ISAC offers network vulnerability assessments, cyberthreat alerts and other related services. As of March, 2022, 24 Vermont school districts were members. Free Tabletop Exercises.