VIRTUAL LEARNING ACADEMY CHARTER SCHOOL
DATA BREACH **EHA**

A. Policy Statement

As a virtual charter school, VLACS treats the personal and sensitive data of its students and staff members seriously. In the unlikely event of data being lost or shared inappropriately, VLACS will take appropriate action to minimize any associated risk as soon as practicable. This policy outlines the steps VLACS will take in response to a data security breach.

B. Types of Breach

A data breach occurs when there is an unauthorized disclosure of an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted per RSA 359-C:19:

1. Social security number.

2. Driver's license number or other government identification number.

3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For students, a data breach also occurs when there is an unauthorized release or access of personally identifiable information. See Policy EHAB for the definition of personally identifiable information.

A breach is not considered to have occurred in the event of unauthorized release or access of information designated as directory information by VLACS in Policy JRA – Student Records – FERPA.

Data breaches can be caused by a number of factors, including, but not limited to, the following:

1. Malicious external attacks such as phishing, social engineering, exploitation of system vulnerabilities, and credential stuffing or brute force attacks;

2. Insider threats such as malicious insiders or privilege escalation;

3. Human error and misconfiguration such as cloud misconfigurations, misdelivery, or unauthorized third-party app usage;

4. Physical security failures such as theft of assets or skimming; or

5. Supply chain attacks such as third-party vendor compromise.

C. Actions to Take in the Event of a Breach

In the event that a VLACS employee discovers a possible data breach, the following steps should be taken:

1. Immediate Containment/Recovery

a. The person who discovers/receives a report of a breach must immediately inform the Information Systems Security Officer, hereinafter referred to as the ISSO. The ISSO is responsible for collecting known pertinent information throughout the incident and finalizing it on the Breach Report Form. If the breach occurs or is discovered outside normal working hours, this should be done as soon as is practicable.

b. The ISSO in consultation with the Chief Executive Officer, hereinafter referred to as the CEO, and relevant members of technology department will ascertain whether a breach has occurred and whether it is still occurring. If so, steps must be taken immediately to stop or minimize the effects of the breach. If a breach has not occurred, the incident may be designated as an inadequate security practice requiring immediate correction.

c. In the case of a breach, VLACS will quickly take appropriate steps to recover any losses and limit the damage, which may include, but are not limited to:

a. Attempting to recover lost equipment;

b. The use of backups to restore lost/damaged/stolen data;

c. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed; and

d. Pausing access to systems for affected users or all users.

2. Investigation into Misuse of Data

In the case of a suspected breach, the ISSO will alert the response team and, based on the nature of the incident, activate members required to investigate the breach. The available response team shall consist of the CEO, ISSO, the administrative team, and the technology team. The response team may assign tasks to appropriate employees to assist with the investigation. The ISSO and activated members of the response team will conduct an investigation to gather all pertinent information about the breach so that the CEO and the school's attorney can determine the likelihood that the information has been misused or is reasonably likely to be misused pursuant to RSA 359-C:20. The investigation should consider, but not be limited to, the following:

1. The type of data;

2. Its sensitivity;

3. What protections are in place (e.g. encryption);

4. How many people are affected;

5. The cause of the breach;

6. What type of people have been affected and whether there are wider consequences to the breach;

7. What has happened to the data;

8. Which individuals have or had access to the data who should not have such access, and, if possible, a description of any possible motivations for such individuals may have for misuse of the information; and

9. The actions taken to mitigate the breach.

The investigation should be completed urgently and, whenever possible, within 72 hours of the breach being discovered/reported.

The ISSO and activated members of the response team will document all mitigation efforts for later analysis. The ISSO will inform the CEO and all relevant members of the response team about the breach, actions taken, and the investigation.

3. Notification

Some individuals, agencies, or both may need to be notified as part of the initial containment and after the investigation is completed.

The CEO, in collaboration with the school's attorney, will use the report generated by the ISSO and activated members of the response team to determine, based on the severity of the breach, whether a legal responsibility exists to notify any individuals, the New Hampshire Attorney General's Office, or both. Pursuant to RSA 359-C:20, notification is required if there is a determination that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made regarding misuse or the potential for misuse. The CEO, the ISSO, or both will inform the response team about the outcome of the meeting with the school's attorney and communicate additional actions if required.

Pursuant to RSA 359-C:20, where there is a determination that a legal obligation to notify an affected individual exists, any notification of a security breach will include the following:

1. A description of the incident in general terms;

2. The approximate date of the breach;

3. The type of personal information obtained as a result of the breach; and

4. The telephonic contact information of an individual on the response team designated to answer the questions and concerns of affected individuals.

In such circumstances where notification under RSA 359-C:20 is required, VLACS will also notify the New Hampshire Attorney General's Office of the breach. This notice will include the anticipated date of the notice to the individuals and the approximate number of individuals in New Hampshire who will be notified. VLACS may report the data breach to the Family Policy Compliance Office, which is not required under FERPA but is considered best practice.

In the case of breaches where there is suspicion of criminal activity, law enforcement may be notified. Every incident will be considered on a case-by-case basis.

In the event that an unauthorized disclosure of a student's data occurs as a result of a breach, VLACS will record the disclosure in the student's education records.

4. Review and Evaluation

After the investigation, the CEO and ISSO will review the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan will be created to minimize the possibility of a future breach. The CEO and ISSO will review this Data Breach Policy after each incident of breach to determine whether modifications to VLACS's breach response strategy are necessary to improve the response process.

D. Implementation

VLACS will notify its staff of this Data Breach Policy. If staff members have any queries in relation to the policy, they should contact the ISSO.

Legal Reference:

RSA 359-C:20 - Notification of Security Breach Required

34 C.F.R. § 99.3, Personally Identifiable Information

Legal References Disclaimer:

These references are not intended to be considered part of this policy, nor should they be taken as a comprehensive statement of the legal basis for the Board to enact this policy, nor as a complete recitation of related legal authority. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

Date Adopted: November 17, 2016

Revision Dates: September 16, 2021; January 20, 2022; July 12, 2022; April 3, 2024; May 5, 2026

Last Review Date: May 5, 2026