VIRTUAL LEARNING ACADEMY CHARTER SCHOOL
DATA SECURITY **EGA**

A. Introduction

This policy is to notify Virtual Learning Academy Charter School, hereinafter referred to as VLACS, employees concerning the appropriate security measures for the handling, storing and transferring of data and information that is owned or maintained by VLACS. This policy will instruct employees regarding the level of security associated with certain data and information. While this policy provides baseline security measures, VLACS and its employees will strive to take appropriate steps to secure and protect information under VLACS' care and control.

B. Scope

This policy applies to employees and any information that is created, stored, and maintained by VLACS. Employees must use appropriate security measures to protect information when accessing VLACS' systems, software, network services, and any other medium in which data is stored and while transmitting data and information. This policy will classify information and instruct employees how to appropriately secure, transfer, and store VLACS data. VLACS specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or intentionally causing any loss of VLACS' data and information. VLACS also prohibits employees from violating any law or breach of confidentiality, or causing any damage to VLACS' computers or network services. Any employee violating this policy may be subject to discipline, up to and including termination of employment. VLACS may issue data security directives from time to time to provide clarification or supplement this policy. Such directives shall be deemed incorporated into this policy.

C. Definitions

All relevant definitions are provided and maintained in VLACS Policy EHAB Data Security and Privacy.

D. Data Classifications

The data and information owned, created, or maintained by VLACS may contain certain private or confidential information. Therefore, employees must maintain awareness of the sensitive nature of the information and data they handle.

VLACS maintains public, confidential, restricted, critical, and personally identifiable data definitions and examples of these different data types in VLACS Policy EHAB Data Security and Privacy.

Only authorized individuals who require that information during the performance of VLACS functions should access Confidential data, Restricted Data, or both. If confidential data must be

accessed across multiple departments or by the entire VLACS organization, the Chief Executive Officer, hereinafter referred to as CEO, or their designee must authorize such access and dissemination. All requests by vendors or third parties for confidential information must be directed to the CEO or designee.

Employees may not discuss or disclose confidential, restricted, or personally identifiable data unless the employee has the requisite authorization from the CEO or designee, or the employee's job duties authorize and require such discussion or disclosure. No employee may release student confidential data or restricted data to unauthorized parties without parental/guardian and/or Chief Executive Officer approval.

All employees must be aware of their responsibilities under the Family Educational Rights and Privacy Act, hereinafter referred to as FERPA, and other relevant federal laws, state laws, and VLACS policies as it relates to accessing and disclosing personally identifiable information, student educational records, and directory information.

Any questions regarding what classification applies to specific data or information should be directed to the CEO or designee.

E. Password Security

Employees must protect their computers from unauthorized access by physically securing them from use by unauthorized persons using a secure password to access the device, by establishing secure passwords for logins, and for accessing VLACS' network services. Employees must maintain sufficiently complex passwords and may be required to change those passwords as requested by VLACS' administrative team or technology team. An employee may not share or reveal any of their passwords unless an employee obtains prior approval from the CEO or designee. In the event of a disclosure of an employee's password to an unauthorized individual, the employee shall immediately notify the Information Systems Security Officer, hereinafter referred to as ISSO, or designee.

Any employees assigned devices by VLACS, including, but not limited to, laptops, desktop computers, and smart phones must also use secure passwords to protect the devices from unauthorized access. Any devices provided by VLACS may not be utilized by any third parties without written permission from the CEO or designee.

F. Data Encryption

VLACS requires that all information transmitted electronically use the appropriate security measures. Data encryption is a procedure used to convert data from its original form into a form designed to prevent an unauthorized third party from accessing the data. Employees must use an encryption or security device when transmitting any confidential information via electronic means, including, but not limited to, HTTPS, SSL, SFTP, and TLS provided the key length is

sufficient according to current standards. Presently, VLACS requires that its employees use Gmail for email transmissions with HTTPS/SSL/TLS enabled when sending or receiving all emails for VLACS business.

Employees should refrain from faxing confidential information unless provided prior authority to do so from an immediate supervisor or the CEO or designee.

G. Backup and Disaster Recovery

VLACS' mission is dependent upon its computer systems and network services. Therefore, in the event of a data loss disaster, VLACS' technology team must respond in a timely and reliable manner to restore VLACS' devices, systems, servers, or any combination of these. Employees must immediately notify the ISSO or designee in the event of any VLACS data loss.

Full backups of VLACS' data must be performed regularly and according to current industry standards. Backup schedules may be adjusted according to

1. The frequency of changes in each set of data; and

2. Storage or other system limitations. Digital storage media containing the backed up information shall be maintained and stored either off-site or according to industry standards for on-site backup storage.

H. Access to Data

Employees shall take appropriate measures to access only VLACS information and data that is necessary to perform their job duties.

Every employee shall:

- Never access or view VLACS data without a valid reason. Access should be on a need-to-know basis.
- Never provide confidential or restricted data to anyone, including, but not limited to, client representatives, business partners, students, parents or even other employees unless the employee has obtained the necessary authority to disclose such information from the CEO or designee.
- Never use VLACS data for training presentations or any purpose other than for performing job related duties.
- Always use secure data transmission methods as defined by this policy and other VLACS policies and physically secured electronic media.
- Always keep confidential information or data only as long as they are needed for VLACS job functions.

- Follow a “clean desk” policy, keeping workspaces uncluttered and securing sensitive documents in locked storage per VLACS policies.
- Always use only approved document disposal services or shred all hardcopy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair, or preparing to reuse electronic media.
- Never allow third parties, including family members, access to confidential or restricted VLACS data.
- Never store confidential, restricted, or personally identifiable data on any non-VLACS issued computer or device unless the employee uses secure password protection and all other reasonable means to prevent third party access.
- Never disclose confidential, restricted, or personally identifiable information on social media or network applications.
- Never post confidential, restricted, or personally identifiable information on VLACS' website.

All requests by third parties for access to VLACS information must be sent to VLACS' CEO or designee.

VLACS' ISSO and technology team employees should ensure that only authorized employees may access confidential, restricted, or personally identifiable information. Employee access protocols should be reviewed annually. Any questions regarding an employee’s authorized level of access to VLACS' information should be directed to the CEO and ISSO.

When an employee’s employment with VLACS ends, Human Resources shall immediately contact the ISSO and technology team leadership for the termination of the employee’s access to VLACS' software, systems, and network services.

I. Physical Security of Servers

In order to maintain the physical security of VLACS' software, systems, and network services, employees may not use other employees’ computers or devices, unless the employee obtains prior approval from the Chief Executive Officer or designee. Employees should refrain from permanently storing VLACS' data or information on their computers or laptops and should instead store such data via VLACS' network services. Temporary copies of data stored on employees’ devices must be deleted regularly.

VLACS' physical infrastructure including, but not limited to, servers room, wiring closets, and servers must be kept locked except when under supervision by authorized VLACS employees during regular business hours as determined by the CEO.

J. Security Breach Response

Data and security breaches and responses are defined in VLACS Policy EHA – Data Breach.

K. Storage of Data and Information

Areas used to store confidential information must be secured by appropriate methods. Computer files must only be accessed by authorized employees and appropriate password protection must be used. Documents containing confidential information must be stored in file cabinets or other means of locked storage. Access to areas containing confidential information must be provided only to authorized employees as determined by the CEO or designee. Data retention and destruction must be in accordance with VLACS' policies and any applicable state and federal laws.

Appendix Reference:

EHA – Data Breach
EHAB – Data Security and Privacy

Legal References:

18 U.S.C. § 2510 et seq. - Electronic Communication Privacy Act (ECPA)
20 U.S.C. § 1232g * Family Educational Rights and Privacy Act (FERPA)

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: March 8, 2012

Revision Dates: May 5, 2026

Last Review Date: May 5, 2026