VIRTUAL LEARNING ACADEMY CHARTER SCHOOL

DATA SECURITY EGA

I. Introduction

This policy is to notify Virtual Learning Academy Charter School (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's care and control.

II. 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's network services and while transmitting information. This policy will classify information and instruct employees how to appropriately secure, transfer, and store that information. VLACS specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or intentionally causing any loss of VLACS's information. VLACS also prohibits employees from violating any law or breach of confidentiality, or causing any damage to VLACS's computers or network services. Any employee violating this policy may be subject to discipline, 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.

III. Definitions

"Confidential data" is information that may be protected by federal and state law or regulations.

"Network services" consists of any configuration of hardware and software which connects users to the VLACS's network, other computers, peripheral devices, or the Internet. Network services include the computer hardware, operating system software, application software, stored data, or any other device or application that allows or assists in the transfer of data within the network or to and from the Internet. Network services also include all devices that allow for the monitoring, security and overall maintenance of the VLACS's network.

"Public data" is information that may or must be open to the general public.

"Restricted data" is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use.

"Security Breach" is any event that causes or is likely to cause confidential or restricted information to be accessed or used by an unauthorized person.

IV. 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 on a day-to-day basis. VLACS classifies such data into the following three categories within this policy:

1. Confidential
2. Restricted
3. Public

“Confidential data” is information that may be protected by federal and state law or regulations. Such information is intended for use only by authorized individuals who require that information during the performance of VLACS functions. If confidential data must be accessed across multiple departments or VLACS-wide, the Chief Executive Officer or designee must authorize such access and dissemination. All requests by vendors or third parties for confidential information must be directed to the Chief Executive Officer or designee.

Examples of confidential data include, but are not limited to:

1. Employee data - includes personnel files, and salary data, insurance data, termination/disability data, appointment data, non-salary related benefits, biographical data.
2. Student data - students’ grade data, biographical, personally identifiable data, academic data, and student record data
3. Parent data - parents’ biographical data or financial data
4. Financial data - financial data of employees, students, and parents
5. Donation data, financial data, employment data, and biographical data
6. Social Security numbers
7. Health information or medical records of students or employees
8. Credit card numbers of VLACS, parents, employees or students

Confidential data must be treated as completely confidential and employees should not discuss or disclose such information with others unless the employee has the requisite authorization from the Chief Executive Officer, or their job duties authorize or require such. No employee may release student information 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 (FERPA) as it relates to accessing and disclosing personally identifiable information, student educational records, and/or directory information.

“Restricted data” is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Restricted data is information that is limited only to members of VLACS who have a legitimate purpose for accessing such data.

Examples of restricted data include but are not limited to:

1. Any information protected under contract
2. Any information VLACS decides not to make public
3. Internal telephone books and directories

4. Any student information that is not otherwise confidential
5. VLACS's student, client, and vendor lists

"Public data" is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data is available to all members of VLACS and to all individuals or entities external to VLACS.

Examples of public data include but are not limited to:

- Publicly posted press releases
- Publicly posted VLACS events
- Publicly available VLACS maps, newsletters, newspapers, and magazines
- Data accessible by the public through the VLACS website

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

V. Password Security

Desktops and laptop computers provide the most vulnerable points of access to VLACS's data and information. Employees must protect their computers from unauthorized access by physically securing them from use by unauthorized persons, and by establishing secure passwords for login, and for accessing VLACS's network services. Employees must maintain sufficiently complex passwords and may be required to change those passwords as requested by VLACS's IT Department. An employee shall not reveal a password to another employee, student, or third party unless an employee obtains prior approval from the Chief Executive Officer or designee. In the event of a disclosure of an employee's password to an unauthorized individual, the employee shall immediately notify the Chief Executive Officer or designee.

Any employees assigned devices by VLACS, such as laptops and/or 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 Chief Executive Officer or designee.

VI. Data Encryption

VLACS requires that all information transmitted electronically via email or the Internet 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; HTTPS/SSL/TLS are examples of satisfactory data transport encryption when 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 Chief Executive Officer.

VII. Backup and Disaster Recovery

VLACS's mission is dependent upon its computer systems and network services. Therefore, in the event of a data loss disaster, VLACS's IT Department must respond in a timely and reliable manner to restore VLACS's computers and/or servers. Employees must immediately notify the Chief Executive Officer or designee in the event of any VLACS data loss that occurs on a VLACS issued computer or other device.

Full back ups of VLACS's 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.

In the event an employee suffers a data loss from a VLACS issued computer or other device, the employee must immediately notify the Chief Executive Officer or designee.

VIII. Access to Data

Employees shall take appropriate measures to access only VLACS information or 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 - client representatives, business partners, students, parents or even other employees - unless the employee knows the identity of that person and has obtained the necessary authority to disclose such information.
- Never use VLACS data for training presentations or any purpose other than for performing job related duties.
- Always use secure data transmission methods (e.g., secure email) and physically secured electronic media (e.g., CDs, USB drives).
- Always keep confidential data (documents and electronic) only as long as they are needed.
- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential or restricted information does not get into the wrong hands.
- 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 information that is classified by this policy as confidential or restricted.
- Never store confidential or restricted 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 or restricted information on social media or network applications.
- Never post confidential or restricted information on VLACS's website.

All requests by third parties for access to VLACS information must be sent to VLACS's Chief Executive Officer or designee.

VLACS's IT Department employees should ensure that only authorized employees may access confidential or restricted information. Employee access protocols should be reviewed annually. Any questions regarding an employee's authorized level of access to VLACS's information should be directed to the Human Resource Manager or Chief Executive Officer.

When an employee's employment with VLACS ends, the Human Resource Manager shall immediately contact the IT Department Manager for the termination of the employee's access to VLACS's computers and network services.

IX. Physical Security of Servers

In order to maintain the physical security of VLACS's computer and network resources, employees must only use those computers or devices assigned to them by VLACS. 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's data or information on their computers or laptops and should instead store such data via VLACS's network services. Temporary copies of data stored on employees' computers and devices must be deleted regularly.

VLACS's servers room, wiring closets, etc. must be kept locked except when under supervision by authorized VLACS employees or during regular business hours.

X. Security Breach Response

Data security breaches include, but are not limited to:

- The distribution of login credentials to other individuals
- Neglecting to log off computers when away from workstations
- Inappropriate or unauthorized dissemination of confidential or restricted data
- Accessing, using, or changing data that are not necessary to perform the individual's regular job duties, or for which the individual has not received express authorization from the Chief Executive Officer or designee
- Third parties that access VLACS network services or computers without authorization

Unauthorized or inappropriate use of data and applications or lack of adherence to security policies and procedures carries serious consequences and may result in disciplinary action, which may include the termination of employment.

If any employee becomes aware of or observes a breach in data or computer security, he/she shall report all such occurrences to the Chief Information Officer, and the Chief Information Officer shall immediately notify the Chief Executive Officer.

In the event of a security breach, the Chief Executive Officer will determine what, if any, actions VLACS will take to comply with applicable law. The Chief Executive Officer will work with other administrators to ensure timely notifications and other legally required responses to those affected by the security breach.

The Chief Executive Officer and the Chief Information Officer may investigate and review the incident with department administrators and may take any appropriate measures to safeguard against future occurrences of similar incidents.

XI. 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 area containing confidential information must be provided only to authorized employees. Data retention and destruction must be in accordance with VLACS's policy and any applicable state and federal laws.

XII. Related Policies and Laws

State and Federal Regulations

- **Family Educational Rights and Privacy Act of 1974 (FERPA)**
  FERPA is the federal privacy law for educational institutions and imposes confidentiality rules and regulations around student educational records. This law prohibits VLACS and its employees from disclosing "personally identifiable education information" such as grades or financial aid information to third parties without the students written permission.

- **Electronic Communication Privacy Act (ECPA)**
  Unlike FERPA and HIPAA, which are specific to certain types of entities, the ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. More specifically, the ECPA imposes liability on any person who intentionally accesses without authorization a facility through which an electronic communication service (email or computer network) is provided, or exceeds an authorization to access that facility, if that person thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage.

Appendix Reference:
Date Adopted: March 8, 2012
Revision Dates:
Last Review Date: