Title: Written Information Security Program (WISP) for Protection of Protected Information
Number: 506
Pages: 6
Date: June 8, 2026

OBJECTIVE

The objective of the development and implementation of this comprehensive Written Information Security Program (WISP), is to create effective administrative, technical, and physical safeguards for the protection of Protected Information and to comply with the Vermont State Colleges' (the "Institution") obligations with applicable regulations.
The WISP sets forth procedures for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Protected Information, in alignment with the VSC Information Sensitivity Policy.
For purposes of this WISP, "Protected Information" includes the following, whether in paper, electronic or other form:

1. Social Security number;
2. driver's license number or state-issued identification card number; or
3. credit card holder data.

The VSC Information Sensitivity Policy includes further examples of Protected Information.

PURPOSE

The purpose of this WISP is to:

1. ensure the security and confidentiality of Protected Information;
2. protect against threats or hazards to the security or integrity of such information; and
3. protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

SCOPE

In formulating and implementing this WISP, the intended scope is to do the following:

1. identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information;
2. assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Protected Information;
3. evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks to Protected Information;
4. design and implement a WISP that puts safeguards in place to minimize those risks, consistent with regulatory requirements; and
5. regularly monitor the effectiveness of those safeguards.

Data Security Coordinator

The Vermont State Colleges has designated the Director of Infrastructure and Information Security to be the Data Security Coordinator. That individual may name an alternate designee in writing. They will be responsible for implementing, supervising and maintaining this WISP, including:

1. initial implementation of the WISP;
2. training of the following persons regarding the WISP and Protected Information security:
    a. all employees;
    b. independent contractors with access to Protected Information; and
    c. any other person involved with the Institution who has or will have access to Protected Information;
3. regular testing of the WISP's safeguards, including backup restoration, tabletop exercises, and penetration tests;
4. evaluating the ability of each of the Institution's third-party service providers to implement and maintain appropriate Protected Information security measures for the Protected Information to which the Institution has permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate Protected Information security measures;
5. reviewing the scope of the Protected Information security measures in the WISP at least annually, or whenever there is a material change in the Institution's business practices that may implicate the security or integrity of records containing Protected Information.

Protections Against Internal Data Security Breach

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

A. Information and Access
    1. The amount of Protected Information collected shall be limited to that amount reasonably necessary to accomplish the Institution's legitimate business purposes, or necessary to the Institution to comply with other state or federal regulations.
    2. Access to records containing Protected Information shall be limited to those persons who are reasonably required to know such information in order to accomplish the Institution's legitimate business purpose or to enable the Institution to comply with other state or federal regulations.
    3. Access to electronic Protected Information shall be restricted to active users and active user accounts only.
    4. Access to electronically stored Protected Information shall be electronically limited to those employees having a unique log-in ID with multi-factor authentication enabled.
    5. The Institution will maintain a list of critical systems, including the type of data stored and transmitted in each system.
    6. Paper or electronic records (including records stored on hard drives or other electronic media) containing Protected Information shall be disposed of only in the following manner:
        a. paper documents containing Protected Information shall be either redacted, pulverized or shredded so that Protected Information cannot practicably be read or reconstructed; and
        b. electronic media or other non-paper media containing Protected Information shall be destroyed or erased so that Protected Information cannot practicably be read or reconstructed.

B. Employees
    1. A copy of the WISP must be distributed to each employee and/or readily accessible on the Institution's website for each employee to access, including part-time, temporary and contract employees, and the Institution expects all employees to comply with the provisions of the WISP and all other record retention responsibilities.
    2. There must be regular training of employees on the detailed provisions of the WISP. The Data Security Coordinator shall organize such training.
    3. Employees are prohibited from keeping unsecured files containing Protected Information in their work area when they are not present, or otherwise failing to take reasonable measures to protect the security of Protected Information. All files and other records containing Protected Information must be secured in a manner that protects the security of Protected Information.
    4. All employees are required to comply with the provisions of the WISP, and if the security provisions of the WISP are violated by an employee, Human Resources shall implement disciplinary procedures in accordance with the Institution's employee handbook or bargaining agreements.

5. Resigned or terminated employees must return all records containing Protected Information, in any form, that may be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.), together with all other records of the Institution.
6. A resigned or terminated employee's physical and electronic access to Protected Information must be revoked when employment ends. Such resigned or terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the premises or information. Moreover, such terminated employee's remote access to Protected Information (such as internet access, e-mail access, voice-mail access) must be disabled in accordance with the VSC Password and Access Management Policy.
7. Employees are expected to report any suspicious or unauthorized use of Protected Information to the Data Security Coordinator as soon as discovered. To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are effective immediately:

Protections Against External Data Security Breach

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are effective immediately:

A. Vermont State Colleges' Computers and Electronic Information Systems
    1. The wireless network at the Vermont State Colleges' locations shall always be encrypted.
    2. All VSC-owned devices used by Institution personnel must be encrypted and password protected.
    3. All portable devices used by employees of the Institution to send and receive their college e-mail shall be password protected, and shall be locked when not in use.
    4. The Institution's computers and computer system, including any wireless system, shall, at a minimum, and to the extent technically feasible, have the following elements:
        a. Secure user authentication protocols including:
            i. control of user IDs and other identifiers;
            ii. a reasonably secure method of assigning and selecting passwords in accordance with the VSC Password and Access Management Policy;
            iii. multi-factor authentication required for login to all critical systems and elevated access;
            iv. restricting access to active users and active user accounts only; and

v. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

b. Secure access control measures that:
   i. restrict access to records and files containing Protected Information to those who need such information to perform their job duties; and
   ii. assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

c. Encryption of all transmitted records and files containing Protected Information that will travel across public networks, and encryption of all data containing Protected Information to be transmitted wirelessly.

d. Reasonable monitoring of systems, including logs of users' activity, for unauthorized use of or access to Protected Information;

e. Encryption of all Protected Information stored on laptops;

f. For Protected Information on a critical system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Protected Information.

g. Reasonably up-to-date versions of system security agent software installed and active at all times, which must include endpoint-protection, and reasonably up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

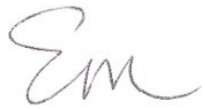
5. New system and application purchases will be reviewed by the IT security team, risks documented, and added to the critical systems list as applicable. In-house developed systems with Protected Information will be similarly assessed.

Protected Information Security Breach

1. Employees must notify the Data Security Coordinator as well as cybersecurity@vsc.edu immediately in the event of a known or suspected Protected Information security breach or unauthorized use of Protected Information.
2. The Institution shall provide notice as soon as practicable and without unreasonable delay when the Institution (a) knows or has reason to know of a Protected Information security breach, or (b) knows or has reason to know that the Protected Information was acquired or used by an unauthorized person or used for an unauthorized purpose. The following notices shall be issued:
   a. Notice shall be provided to the individual(s) whose information was acquired or otherwise affected by an unauthorized person.
3. To the extent required by applicable regulations, notice shall be provided to the state Attorney General and other required regulatory bodies. Such notice shall include the

nature of the breach of security or unauthorized acquisition or use, the number affected by such incident at the time of notification, and any steps the Institution has taken or plans to take relating to the incident, or other information required by law or regulation. Whenever there is a Protected Information security breach or unauthorized use of Protected Information, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the Institution's security practices are required to improve the security of Protected Information for which the Institution is responsible.

Signature:



Dr. Elizabeth Mauch, Chancellor