Chippewa Valley Technical College

Gramm Leach Bliley (GLB) CVTC Information Security Plan

Overview

The Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, CVTC has adopted an Information Security Program for certain highly critical and private financial and related information. This security program applies to customer financial information (covered data) the College receives during business as required by GLBA as well as other confidential financial information the College has voluntarily chosen as a matter of policy to include within its scope.

Covered data and information.

Includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the College chooses as a matter of policy to also define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received during business by the College, whether such financial information is covered by GLBA. The covered data and information include both paper and electronic records.

Annual Board Reporting

CVTC's Information Security Officer will periodically report to the district board regarding the information security plan.

Information Security Plan

This Information Security Plan describes Chippewa Valley Technical College's program to protect information and data in compliance with the Financial Services Modernization Act of 1999, also known as the Gramm Leach Bliley Act, 15 U.S.C. Section 6801, including the GLBA Safeguards added in 2023. The components of the Information Security Policy containing said safeguards are the following:

- designating an employee or office responsible for coordinating the program;
- conducting risk assessment to identify reasonably foreseeable security and privacy risks;

- ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored;
- vendor evaluation and security compliance;
- disclosure of covered data breaches in accordance with the Student Aid Internet Gateway Agreement (SAIG)
- maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems;
- Maintaining a written incident response plan;
- Reviewing access controls, assessing application development and safely disposing of data

Security Plan Coordinator

The Chief Information Officer, in consultation with advisory staff, is responsible for the maintenance of information security and privacy. Advisory staff includes but is not limited to the Network Services and Infrastructure Manager, CVTC Executive Cabinet, Risk Assessment Committee, professional security contractors and Information Security Insurance providers.

Risk Management

CVTC recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security because of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems

- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

CVTC recognizes that this may not be a complete list of the risks associated with the protection of Protected Information. Since technological growth is not static, new risks are created regularly. Accordingly, the CVTC Network Operations Team and Chief Information Officer will actively participate with and seek advice from the Risk Management Committee and professional information security contractors to maintain knowledge of the current threat landscape. CVTC believes current safeguards used by the Department of Information Security at the College are reasonable and, considering current risk assessments are sufficient to provide security and confidentiality to Protected Information maintained by CVTC.

Risk Assessment

CVTC will engage with a third party annually to conduct an objective risk assessment based on the security controls outlined in the Gramm Leach Bliley Act.

Information Safeguards

The Information Security Program will verify that information safeguards are designed and implemented to control risk

1. **Inventory**

   The Department of Information Technology maintains information systems capable of automatically tracking a dynamic environment. When necessary, a detailed inventory of applications, infrastructure and associated services can be produced.

2. **Employee Training**

   The coordinator agrees to work with responsible parties to ensure that adequate training and education is developed and delivered to all employees with access to the covered data.

3. **Information Systems**

Information systems include network infrastructure, applications and related components involved in the processing, storage, transmission, retrieval or disposal of data.

The coordinator, in conjunction with Network Services and Enterprise Applications Team will ensure that the design and operations of network and software systems will reasonably limit exposure to risk.

Specific mechanisms may include but are not limited to:

- Intrusion prevention and firewall solutions
- Routine third party penetration testing
- Routine internal and external vulnerability scans
- Multi-Factor authentication (for all user accounts without exception)
- Data Encryption (both in transit and at rest)
- Security Information and Event Management (SIEM)
- Data Loss Prevention
- Malware Protection
- Anomalous Behavior Detection and Remediation
- Least Privileged Access
- Incident tracking and response platforms
- Change auditing and management systems
- Background Checks
- Anti-Malware
- DNS Exfiltration Prevention
- Adherence to the NIST Cyber Security Framework and NIST SP 800-122

4. **System Failure Monitoring and Management**

The CVTC Department of Information Technology will maintain solutions effective at preventing, detecting and responding to attacks and other system failures.

5. **Vendor Evaluation and Security Compliance**

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources to Chippewa Valley Technical College. In the process of choosing a vendor it is the duty of the CVTC employee acquiring services to ensure that any agreements include the following provisions:

a. A stipulation that PII will be held in strict confidence and accessed only for the explicit purpose of the contract

b. Written verification that the vendor or agency follows any policy or regulations relevant to the data. This includes but is not limited to FERPA, PCI, HIPAA, GPDR, GLBA and ADA.

c. Evidence that reasonable security safeguards are in place to prevent data loss or incidental exposure

6. **Access Control Review**

The CVTC department of Information Technology will maintain solutions, processes and procedures to periodically review access controls using the least privileged zero-trust model.

7. **Application Development Assessment**

CVTC will maintain processes and procedures for routinely assessing the security of in-house and third-party applications that encounter customer data.

8. **Secure Disposal**

CVTC ensures secure disposal of customer data via retention policy and equipment/media destruction practices.

9. **Change Management**

The CVTC department of Information Technology reviews, audits, monitors and records change to information systems and network infrastructure.

10. **User Activity Logging**

The CVTC department of Information Technology maintains various solutions to monitor and log user activity across all systems and infrastructure with the ability to target suspicious activity.

Federal Aid Applicant Information and Breach Disclosure

In accordance with the Student Aid Internet Gateway Agreement (SAIG) CVTC ensures that Federal Aid applicant information is protected from access by or disclosure to unauthorized personnel. In the event of a data breach exposing said information to unintended parties the Security Plan Coordinator will notify Federal Student Aid at CPSSAIG@ed.gov.

Program Maintenance

This program is evaluated and adjusted continuously. Feedback from risk assessments, covered units and security operations are incorporated and considered in the selection and implementation of program components and safeguards by the program coordinator.

Related Policies and Procedures

CVTC maintains a public repository for consumer disclosure. Policies and procedures related to the GLBA Information Security Policy can be found at https://www.cvtc.edu/about-cvtc/consumer-disclosures.