Gramm-Leach-Bliley Act (GLBA) NWTC 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.). NWTC has adopted an Information Security Program to safeguard sensitive data and meet GBLA requirements.

This security program applies to customer financial information (covered data) that the College receives during normal business as required by GLBA as well as other protected 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 sensitive data outlined in the NWTC Sensitive Data Policy.

Information Security Plan

This Information Security Plan describes Northeast Wisconsin 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. 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;
- 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;

Security Plan Coordinator

The Chief Information Officer, in consultation with advisory staff, is responsible for information security, and privacy. Advisory staff includes but is not limited to the Technical Director of Infrastructure and Client Services, information security analysts, and the NWTC Executive Leadership Team.

Risk Management

NWTC 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
- Accidental disclosure of covered data and information

NWTC recognizes that this may not be a complete list of the risks associated with the protection of covered data. Since technology growth is not static, new risks are created regularly. Accordingly, the Information Security Analyst and supporting teams will actively research and test new safeguards provide additional security and confidentiality to covered data maintained by NWTC.

Information Safeguards

The Information Security Program utilizes various safeguards including, but not limited to, the following:

1. Inventory

The Division of Information and Instructional 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 Information Security Analyst agrees to work with responsible parties to ensure that adequate training and education is developed and delivered to all employees with access to covered data, which includes intermittent phishing assessments, new employee orientation, Hub resources, news articles, mandatory FERPA training, etc.

3. Information Systems

Information systems include network infrastructure, applications and related components

involved in the processing, storage, transmission, retrieval or disposal of data.

The Information Security Analyst, in conjunction with the Infrastructure Services and Enterprise Applications Teams will ensure that the design and operation of information systems will reasonably limit exposure to risk.

Specific mechanisms may include, but are not limited to:

- Intrusion prevention and firewall solutions
- Third party penetration testing
- Routine internal and external vulnerability scans
- Multi-Factor authentication
- Data Encryption (both in transit and at rest)
- Security Information and Event Management (SIEM)
- Data Loss Prevention
- Anomalous Behavior Detection and Remediation
- Least Privileged Access
- Incident tracking and response platforms
- Change auditing and management systems
- Background Checks
- Anti-Malware Protections
- Adherence to the Center for Information Security (CIS) Critical Security Controls Framework
- Email Protections (SPF, DMARC, anti-spoofing/phishing)
- Collection of internal threat intelligence
- Internal risk assessments and threat hunting
- Sensitive Data Policy and Procedures for safeguarding sensitive data

4. **System Failure Monitoring and Management**

   The NWTC Division of Information and Instructional Technology will maintain solutions effective at preventing, detecting and responding to attacks and other system failures, Federal Aid Applicant Information and Breach Disclosure

In accordance with the Student Aid Internet Gateway Agreement (SAIG) NWTC 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 Information Security Analyst 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

NWTC maintains a public repository for consumer disclosure. Policies and procedures related to the GLBA Information Security Policy can be found on our website.