IT 04 Standards for Safeguarding Customer Information (GLBA)

I. PURPOSE

This document summarizes West Shore Community College's (the College) comprehensive written information security program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act (GLBA). Specifically, this document addresses § 16 CFR 314.4 -- Elements (the Program) and describes the Program elements pursuant to which the College intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to students. The Program incorporates by reference the College's policies and procedures enumerated below and is in addition to any College policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA, GLBA, GDPR, and FTC – Red Flag Policies.

The Program applies to any record containing nonpublic financial information about a student, or other third party who has a relationship with the College, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student, or other third party provides to obtain a financial service from the College, (ii) about a student or other third party resulting from any transaction with the College involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

II. BACKGROUND

III. AUTHORITY

Board Policy 1050 - Data Security
Board Policy 2028 – College Procedures

IV. DEFINITIONS

Each letter, (a), (b), (c), etc. under the V. Procedure section corresponds with the same section of § 16 CFR 314.4 -- Elements of the Program.

Customer Information – Any record containing nonpublic personal information about a customer of this College.

V. PROCEDURE

§ 314.4 Elements:

(a) West Shore Community College's Director of Information Technology is designated as the qualified individual (program officer) responsible for overseeing, implementing, and enforcing the information security program for West Shore Community College. The program officer may designate other representatives of the College to oversee and coordinate elements of the Program.

(b) The College's Information Technology Department utilizes the Center for Internet Security (CIS) Critical Security Controls as the basis for all technology and customer risk assessment and security. The CIS Critical Security Controls are reviewed annually to ensure compliance.

The College has in place a Cyber Incident Response Plan to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of West Shore Community College Information System Resources and college data. This adverse event may be malicious code attack, unauthorized access to college systems, unauthorized use of college services, denial of service attacks, general misuse of systems, and accidental loss or hoaxes. In addition, the following security measures have been implemented:

- Account locking – Five bad consecutive password attempts will result in the user's account being locked for 15 minutes. This lockout triggers an alert to the WSCC network team.
- An anti-virus application is installed on all workstations and servers to monitor for viruses and malware.
- Network monitoring and alerts notify the network security team of accounts that have been compromised or a compromise attempt. Compromised accounts are then investigated to determine the severity of the threat. If necessary, the user is required to change his or her password.
- A password procedure that identifies minimum standards for user passwords; see I.T. department procedure "IT09 - WSCC Information Technology Procedure."
- Additional risk testing is conducted through internal and external penetration tests by an external vendor (see paragraph d2ii).

(c) Access to physical servers is limited by lock and key. Access to virtual servers is limited by user permissions and further limited to Information Technology personnel only who have been granted those permissions.

Access to customer information is controlled using Microsoft Active Directory, the Student Information System application, and the document storage system with position-based permission groups. Permissions are granted to new employees based on positional roles within the College. User accounts are locked immediately after employee termination and all permissions are removed from the terminated user's account. All permission access requests are documented through the Information Technology Department's Helpdesk ticketing system.

Audits of access to customer data are performed regularly by the Enterprise Database Administrator. Audits include but are not limited to access logs to the primary database, event logs of the Student Information System application and servers, and access logs of the college's primary financial access application.

All business financial data is transmitted to and from the financial end points via SSH File Transfer Protocol encryption. Encryption of the primary customer database is not currently supported by the application's vendor. All email transmissions are encrypted via Microsoft 365 encryption methods.

Student access to their specific information is limited to those with an active student user account using a username provided by the College and a secure password set by the student. Access is made through the campus portal using a secure URL using HTTPS.

West Shore Community College does not develop applications that transmit, access, or store customer information.

The College has in place Multi-Factor Authentication (MFA) for all employees and active students to add a layer of security in limiting unauthorized access to all customer systems.

All customer (student) user accounts are disabled 24 months after the student last enrolled at the college. All user accounts (non-student) are disabled immediately upon termination. Disabling the user account disconnects the user from being able to access all WSCC systems including any PII (See Information Technology Department Knowledge Base Article "Admin-Employee Termination Process").

The disposing of customer data is not reasonably feasible due to the need to access historical information by the organization or the possible re-enrollment of a student (customer) later. User accounts are never deleted, only archived.

When necessary to replace a physical device that may have contained customer information, the college follows the process as outlined in the Information Technology Department Knowledge Base Article titled: “Hardware-Hard Disk Sanitation Process”.

Data and record retention processes are defined in the College’s Business Office procedure, #BUS 34.

The College uses a change management log to track changes to the network infrastructure.

The College utilizes firewall intrusion protection and notifications along with security access monitoring to provide alerts of attempted unauthorized access to the WSCC internal network.

(d) The Network Security Team uses several software applications to continuously monitor the network and data infrastructure for internal and external threats and vulnerabilities. Applications are also installed on workstations and servers to aid in early threat detection. Threats and vulnerabilities are evaluated by team personnel and addressed as deemed appropriate based on the severity of the threat. All identified threats and the remedial action taken to address those threats are logged. Additionally, all changes to the network and data infrastructure, such as reconfiguration of security policies, addition or removal of equipment, or physical changes to the infrastructure are also logged by the appropriate department personnel.

Internal and external penetration tests are conducted annually. Penetration test results are reviewed by the Information Technology Security Team and non-compliances are addressed.

To mitigate risk to the network, data and end-users, the College’s Information Technology Department has systems in place to provide user workstations and servers with regularly scheduled operating system security patches and updates.

Vulnerability and threat assessments are conducted, at a minimum of, twice per year by the Network Security Team. Vulnerability and threat assessment consists of the review of all incidents that have taken place along with a review of any network and data infrastructure changes since the last assessment was conducted. Adjustments, changes, additions and deletions to the network security policies and procedures may be made according to assessment findings.

(e) The College has in place polices and procedures to ensure that personnel can enact the information and data security program. The College provides security training for all new employees and continuous training for current employees.

The Department of Information Technology has an information security team that consists of the Director, Network Administrator, Computer and Media Services/Network Technician and the Computer and Media Services Technician that oversee the network and data security. Members of the security team continuously monitor and manage security risks and assess threats.

(f) The College maintains policies (Board Policy 6010 - Purchasing) and procedures (06 ADM Purchasing) that identify purchase standards and proper vendor selection. Additionally, the College's Information Technology Department has further identified criteria for the selection and retainment of third party managed service providers; see I.T. department procedure "IT05 - Managed Service Provider Selection and Retention."

(g) The Information Technology Security Team annually reviews its information security program and adjusts security systems based on findings of audits, recommendations of service providers, testing, recommended industry security guidelines, direct attack cyber-incidents. All changes to the security program are documented in the Network and Data Security Program Review Log.

Approved: mm/dd/year