501.6 SECURITY OF FINANCIAL INFORMATION

Warren County Community College is subject to various federal requirements to secure the financial information of students. Policy 501.6 enumerates the actions that the College will continue to undertake to secure financial information.

501.6.1 GRAMM-LEACH-BLILEY ACT

Under the 2000 Gramm-Leach-Bliley Act (G-L-B Act), the College is considered a financial institution because two of the College's activities ("making, acquiring, brokering, or servicing loans" and "collection agency services") are consistent with banking industry functions under the Bank Holding Company Act of 1956. As a result, the College must comply with two requirements of the G-L-B Act: Privacy of Consumer Information (Privacy Rule) and Safeguarding of Consumer Information (Safeguards Rule).

A) Privacy of Consumer Information

The privacy of student information contained in the G-L-B Act is consistent with the privacy responsibilities that colleges and universities must follow under Family Educational Rights and Privacy Act (FERPA). As such, Warren Community College will continue to ensure the privacy of student records, including their financial records, under Policy 306: Privacy Rights of Students, to satisfy the Privacy Requirements of the G-L-B Act. In addition, where applicable, the College shall comply with the safeguards of information for students covered under the General Data Protection Regulation (the European "Right to be Forgotten" law).

B) Safeguarding of Consumer Information

WCCC is committed to safeguarding the financial information of students and members of the campus community. As such, it has developed the following standards to safeguard financial information for students and employees (hereafter "customers"):

1) Electronic Safeguards

a. Electronic customer information is stored on secured servers. All servers are password protected and unauthorized access is protected via a series of firewalls and other protections. Network security is routinely tested and subject to security audits.
b. Servers are routinely backed-up and the back-up information is stored off-site.
c. Employees are advised to maintain all work product on network drives to ensure that materials are backed up daily.
d. Anti-virus software is routinely used. Security patches are installed as necessary, according to the latest industry standards.
e. As specified in Policy 201.15, all non-student employees are subject to employee criminal background checks.
f. Each employee and student with computer access is issued a unique ID and password. Employees must change passwords periodically using a specific password protocol to minimize the potential of "hacking" and must ensure that all passwords are secured.
g. The College limits access to various computer systems to employees requiring such access for the completion of their job duties.

h. Employees with access to secure student information must implement a keyboard locking protocol to secure information when they are away from their workstations.
i. The College has a system of "permissions" and "controls" in place to limit both inquiry and data entry access to various systems and system components to protect from unauthorized access to confidential information.
j. All data are erased when disposing of computers and other electronic media that contain customer information.
k. Effective disposal of hardware occurs after the completion of its useful life cycle. The College maintains a comprehensive inventory of its technology equipment.
l. Employees with laptops containing sensitive data must follow the protocols in the Secure Laptop Policy (Policy 202.20), including the use of encrypted laptops or thumb drives if secure data are taken off campus.
m. The College's contracted vendor provides assurance that there is effective erasure of all confidential scanned data from photocopiers.
n. The College and/or its contracted vendors ensure that confidential data are maintained and disposed in accordance with state records retention statutes.

2) Physical Safeguards

a. Access to the server room is restricted to certain employees issued electronic key fobs. The room remains locked at all times and has been fortified with additional physical protection.
b. Rooms and/or file cabinets containing paper records with confidential customer information are locked.
c. Fireproof cabinets are used to store student records, financial aid files and employee financial information.
d. All employees are trained to safely dispose of confidential information using shredders or special disposal bins.
e. Any confidential material not shredded on campus is disposed of by a bonded confidential data disposal agency.
f. Confidential materials not housed on campus are stored off-site at a bonded storage company. Records are retained in accordance with federal or state records retention requirements and are destroyed after the retention period.

3) Other Safeguards

a. Financial account information is not provided over the telephone or in-person, unless or until an individual can produce sufficient identification.
b. The College limits employees who may accept financial information (example: credit card numbers) and does not keep permanent records of student financial information.
c. The College outsources payment plan, credit card processing and payroll activities to external vendors and receives assurances from these vendor that they are in compliance with all federal and state mandates.
d. Social security numbers are not used for student identification. Social security information is collected only for federal or state mandated purposes, such as financial aid filing or tax reporting.
e. Signed releases or court-mandated documents are required for the release of FERPA covered information.

f. The College has developed Emergency Action, Disaster Recovery and Business Continuity Plans/Procedures. Offices are responsible for periodically updating these documents.
g. The College's internal controls and operating procedures are reviewed annually by an independent auditing firm.

Approved: 5/20/09
Revised: 2/27/2013
Revised: 9/16/2020