WALLA WALLA COMMUNITY COLLEGE
PCI-DSS COMPLIANCE
ADMINISTRATIVE POLICY 8250

I. POLICY BACKGROUND/PURPOSE

This policy defines the safeguarding of cardholder data that is stored, processed, or transmitted.

II. AUTHORITY

Board Policy 1370. This policy is a component of the Walla Walla Community College (WWCC) information security program that is intended to comply with the PCI-DSS, FERPA, Gramm Leach Bliley Act (GLBA) and other regulations.

III. SCOPE OF POLICY

This policy applies to all areas where Payment Card Industry (PCI) cardholder data (CHD) is stored, processed, and/or transmitted, and all relevant employees and third-party agencies who handle CHD.

IV. DEFINITIONS

A. **Payment Card Industry Standard Data Security Standard (PCI DSS)** - A set of security standards that was formed in 2004, jointly created by VISA, MasterCard, Discover Financial, JCB International, and American Express. The standards are aimed to secure credit and debit card transactions against fraud and theft. It is a requirement for any business that processes credit or debit card transactions.

B. **Cardholder data (CHD)** - Any personally identifiable information (PII) associated with a person who has a credit or debit card. CHD includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date, or service code.

C. **Cardholder Data Environment (CDE)** - A computer system or networked group of IT systems that processes, stores, and/or transmits cardholder data or sensitive payment authentication data. A CDE also included any component that directly connects to or supports this network.

D. **System Components** - Any network component, server, or application that is included in or connected to the cardholder data environment (CDE). For example, the following types of systems would be in the scope for compliance within any environment:

   1. Systems storing CHD
   2. Systems processing CHD
   3. Network devices transporting or directing cardholder traffic (e.g. border router, Firewall, wireless networking equipment, etc.)
   4. Devices that create media containing CHD.
   5. Support systems (e.g. Active Directory, syslog server, IDS, desktop/laptop performing support functions such as system administration, etc.)

V. POLICY

A. Cardholder Data Storage

   1. It is forbidden to store PCI-DSS data on any storage media.

2. IT equipment that has been deployed in the cardholder data environment (CDE) and is no longer needed for business or legal reasons will be decommissioned. All paper-based records of CHD will be destroyed by cross shredding.

A. Hardware Inventory
   1. Inventories will be kept of all PCI-DSS hardware where CHD is stored, processed, and/or transmitted. This inventory will be maintained and reviewed at least annually.
   2. The inventory will detail the following information:
      a. Device make
      b. Device model
      c. Device serial number
      d. Device location

B. Device Inspections
   1. Each department manager shall inspect devices that capture CHD on a regular basis to detect tampering or substitution. This shall be done via visual inspection and by checking the serial number or any other device characteristics to verify it has not been swapped with a fraudulent device or tampered with.
   2. A media inventory log shall be kept to monitor the device inventory.
   3. Each department manager must ensure training is provided to all staff that captures, processes, or transmits CHD as part of their business functions. Annual review of this training material will be carried out by the department manager.
   4. Staff handling CHD will be trained to ensure they can monitor the following:
      a. Verifying the ID of any 3rd party maintenance
      b. Verifying installation/removal of devices
      c. Awareness and reporting of any suspicious behavior
      d. Ensure any tamper tape added to the devices has not been tampered with.

D. Exceptions
   1. Only the President of WWCC or a designated appointee is authorized to grant exceptions to this policy.

V. COMPLIANCE

To ensure compliance with this policy, WWCC may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any WWCC information resources, consent to disclosing the contents of any files or information stored or passed-through WWCC's network and may be subject to monitoring.

A. Enforcement
   1. Personnel and students using WWCC's information resources in opposition to this policy may be subject to limitations on the use of these resources, suspension of privileges (including internet access), as well as disciplinary and/or legal action, including termination of employment, or suspension of enrollment.
   2. Employees, contractors, consultants, temporaries, partners, and all personnel affiliated via third parties shall sign an agreement to comply and be governed by this policy and the WWCC Information Security Policies upon hire and must be reviewed annually.

B. Violations
   1. In conjunction with the Vice President of Human Resources, a Supervisor, Department Supervisor, Dean, or Vice President will address employee violations of this policy.
   2. The Vice President of Student Services will address student violations of this policy in accordance with the Student Code of Conduct.

VI. REFERENCES

A. PCI DSS Quick Reference Guide

Policy Contact: Vice President of Administrative Services
Approved by (Department/Body): Dr. Chad Hickox, President
Date Originally Approved: December 16, 2025
Last Reviewed/Revised on: