WALLA WALLA COMMUNITY COLLEGE
INFORMATION PROTECTION
ADMINISTRATIVE POLICY 8400

I. POLICY BACKGROUND/PURPOSE

The purpose of this policy is to define how information is stored, processed or transmitted electronically, or on hardcopy must be protected at Walla Walla Community College (WWCC) from unauthorized access or disclosure. Controls must be in place to ensure confidentiality, integrity, and availability of information.

II. AUTHORITY

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

III. SCOPE OF POLICY

This policy applies to all electronic and hardcopy information. This encompasses non-public information which should not be disclosed outside the College as well as information with limited disclosure within the College. This coverage includes all such non-public information physically located at WWCC or located off-site including cloud computing, cloud storage, third-party service providers and offsite storage.

IV. POLICY

A. Information systems storing, processing, or serving non-public information, as defined by Washington State OCIO Data Classification Standard 141.10 (4.1), will be secured with logical and physical access controls. Physical access controls will be used to restrict access to hardcopy non-public information.
B. Logical access to electronic information will be granted only with approval by the user's manager granting them the minimum level of access required for their job responsibilities.
C. Physical access controls shall be used to restrict physical access to information systems storing non-public information, to areas storing non-public hardcopy information, and offices where the public is not allowed without an escort and a log of their visit.
D. Non-public hardcopy information must be protected and stored in locked cabinets or locked rooms when not in use especially outside of office hours. Locked offices may not provide sufficient protection as cleaning and/or facilities maintenance staff may have access.
E. Non-public hard copy information will not be copied or faxed from equipment not owned and/or operated by the College.
F. The rules for handing non-public information are outlined below:
    1. Users that have access to confidential or sensitive information must have a background investigation check.
    2. Third parties that have access to confidential information must be contractually obligated to comply with the appropriate privacy and security laws, regulations and standards for the information including, Gramm-Leach Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Federal Educational Rights and Privacy Act (FERPA).

3. Non-public information should only be printed or faxed when required for business, legal or regulatory purposes.
4. Care should be taken when printing non-public information to printers configured for general office use, secure print should be used where possible.
5. Printouts and fax receipt of non-public information should be retrieved immediately, unless secure print is implemented.
6. Fax transmissions of non-public information should be made only if the recipient is confirmed to be physically present at the receiving fax machine, unless secure faxing is being used.
7. Unencrypted confidential and sensitive information must never be sent by end-user messaging technologies such as e-mail, instant messaging and chat.
8. If transmission of any confidential or sensitive information is necessary via e-mail, strong encryption must be used and passwords and/or keys must not be transmitted together with the information.
9. Non-public information is not to be released unless prior approval is received from management and without authorization from the person whose information has been requested.
10. Non-public information will be securely disposed of when no longer needed.
11. Any information restricted from storage by applicable security and privacy laws, regulations and standards such as payment card magnetic stripe full content or its Card Verification Code Value (CVV2, CVC2, CID, CAV2) will not be stored in electronic or hardcopy form.
12. Encrypt confidential and sensitive information such as payment card Primary Account Number (PAN) or Social Security Number (SSN) using industry standard cryptography and security protocols to safeguard the information during storage and transmission.
13. Confidential and sensitive data will be masked when displayed for all data, except where there is a business need to view the information.
14. Any confidential or sensitive information required for testing purposes must be sanitized before being used in development or testing.
15. Encrypted confidential and sensitive information stored on laptops, USB devices, mobile devices, and other portable media will be allowed only if there is legitimate business need and no alternative exists.
16. All backups of non-public information must be encrypted using industry standard encryption techniques.
17. Distribution of any off-site media containing encrypted confidential or sensitive information should be approved by management.
18. Information that is accessible on the internet for staff, customers, vendors, partners, agencies, etc. will be protected by a firewall.
19. Hardcopy non-public information should only be taken off the premises if there is a legitimate business need, management approval, and the user maintains possession of such documents at all times.

G. All media used to store organizational data will be sanitized in accordance with NIST SP 800-88 Rev. 1.
H. 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.

V. REFERENCES

RCW 42.56.590

Policy Contact: Vice President, Administrative Services
Approved by (Department/Body): Dr. Chad Hickox, President
Date Originally Approved: July 16, 2024
Last Reviewed/Revised on: _____