WALLA WALLA COMMUNITY COLLEGE
ACCESS CONTROL
ADMINISTRATIVE POLICY 8410

I. POLICY BACKGROUND/PURPOSE

The purpose of this policy is to control access to Walla Walla Community College's (WWCC) applications, systems, hardware, and the execution of automated functions.

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 users, including but not limited to students, faculty, staff, contractors, and visitors of WWCC IT resources and data.

IV. POLICY

A. Access to specific applications shall be granted to personnel with legitimate need. Privileges assigned shall be limited to the minimum required to perform assigned duties. All access not explicitly authorized is forbidden.
B. A segregation of duties will exist between an individual with authority to determine who has access to WWCC resources and the individual assigning the access rights.
C. Access to confidential information will require both a unique username, password, and a required multifactor authentication.
D. Access to confidential hardcopy information will be protected by physical controls.
E. Administration / System Administrators shall:
    1. Update access rights based on any changes.
    2. Review user access rights every six (6) months, and modify, revoke, or deactivate as appropriate.
    3. Create and administer accounts for specific individuals and not allow any shared, group, or generic accounts for access to data. If such accounts are built-in to applications they will be disabled if possible.
F. When a termination or transfer of personnel occurs access rights will be revoked and/or realigned as appropriate.
G. Users are accountable for all activity associated with their username, password, and must never share their personal login credentials.
H. No generic or shared user ID's will be created or used, and the reuse of a user ID is not allowed after an employee or student terminates their relationship with WWCC.
I. Passwords will be changed if there is a suspected compromise of credentials.
J. Computer and communications system privileges will be restricted to a need to know basis.
K. Access control to computing systems must be configured to lock after a period of inactivity.
L. Accounts will be disabled after multiple failed login attempts.
M. All user accounts that are inactive over ninety (90) days will be archived.
N. Users will not circumvent access rights in order to gain access to unauthorized information resources.

O. Users will not allow anyone else to use their accounts or use their computers.
P. 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

Washington State OCIO Policy 141.10

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