

WALLA WALLA COMMUNITY COLLEGE
IT THIRD-PARTY SERVICE PROVIDER MANAGEMENT
ADMINISTRATIVE POLICY 8210

I. POLICY BACKGROUND/PURPOSE

The purpose of this policy is to describe the information security requirements to be followed in the selection and management of IT third-party service providers at Walla Walla Community College (WWCC). This policy also defines the information security requirements for contracts with third-parties.

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) and other regulations.

III. SCOPE OF POLICY

This policy applies to all engagements with service providers.

IV. POLICY

- A. Arrangements involving third-party access to information processing facilities or assets shall be based on a formal contract. The contract will contain, or reference, all security requirements and the assigned responsibilities to ensure that there is no misunderstanding with the third-party.
- B. Sponsors and owners of outsourced business functions shall exercise appropriate due diligence in the selection of the service provider.
- C. The service provider implements appropriate security controls in accordance with organizational policies.
- D. Services provided by the service provider shall be monitored to confirm that they are in compliance with the contract.
- E. When the service provider requires access to confidential information, it is IT's responsibility to ensure that the contract includes requirements for data confidentiality.
- F. All accounts used by vendors for remote maintenance will be enabled during the duration of the contract only.
- G. Exceptions
 - 1. Only the WWCC President 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

[RCW 19.255.010](#), [RCW 42.56.590](#)

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