WALLA WALLA COMMUNITY COLLEGE
IT PHYSICAL AND ENVIRONMENTAL SECURITY
ADMINISTRATIVE POLICY 8420

I. POLICY BACKGROUND/PURPOSE

The purpose of this policy is to define information security requirements to prevent unauthorized access, damage, and interference to physical premises, information and sensitive assets.

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. DEFINITIONS

A. *Datacenter* – the server room where all centralized IT machines and campus network equipment reside.

IV. SCOPE OF POLICY

This policy applies to all WWCC premises where critical IT systems are located and which will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

V. POLICY

A. College equipment will be installed in suitably protected areas with minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.

1. The datacenter entrance locations containing critical IT systems will be locked when unattended and protected during non-business hours with monitoring via security cameras.
2. Physical access controls such as locks, keys, and swipe cards will be used to protect critical IT systems and infrastructure.
3. Datacenter back-up media will be stored at an alternate location.
4. Datacenter access will be restricted to authorized IT personnel.
5. Effort must be made to protect against fire, flood, and other environmental factors.

B. Visitors

1. Support services personnel are granted access to secure areas only when required, authorized, and supervised. The IT employee hosting the visitor must come to the reception area for Technology Services, have the visitor sign in to the Visitor Log Book, documenting their name, and purpose of the visit. Visitors are to be issued a badge identifying the individual as a visitor.
2. Upon the completion of the visit, the visitor must sign out in the Visitor Log Book and return their badge.

C. 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.

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