

# Computer Center Access & Maintenance

## University Operations – Information Security

### CWU Policy 204-07

**Effective:** February 11, 2015

**Policy Review Date:** YEAR

**Policy Executive:** Chief of Staff

**Responsible Office/Unit:** Information Services and Security

#### **Policy Statement:**

#### **Applicability:**

---

#### **Content:**

Policy

Appendix A – Computer Center Access & Maintenance Procedure

---

#### **(1) Policy**

- A. The purpose of this policy is to ensure the physical security of the CWU Computer Center (CWUCC) which houses the central computing resources for the university including the Computer Operations Center, Network Operations Center and Telecommunications Center.
- B. All personnel requiring access to the CWUCC who are not permanently assigned to the CWUCC are to register at the main Operations Desk.
- C. The name and location of the CWUCC will remain anonymous to the greatest extent possible. The building, physical location, and other identifying characteristics will remain anonymous in order to protect the location from unauthorized access and activities. All references are protected from public disclosure as critical computing assets pursuant to RCW 42.56.420.
- D. In the event of an emergency situation during hours when the CWUCC is not staffed, authorized personnel requiring access may do so without notification. Emergency situations are limited to events which are highly likely to adversely impact the operational integrity of the CWUCC or may result in equipment damage or personal injury. Personnel are to register and notify IS operations staff at the earliest convenience with the specifics of the emergency and any actions taken.

- E. Only personnel with a business need to enter the facility are granted access. IS management and/or its delegated staff is authorized to deny access to any individual who does not have a business need or who violates this policy. Policy violations will lead to disciplinary action.

## **(2) Scope**

- A. This policy applies to the physical access of the CWUCC and is applicable to all students, faculty, staff, student employees, and outside contractors that are affiliated or conduct work on behalf of the University.

## **(3) Responsibilities**

- A. The Chief Information Officer (CIO) or other designee is responsible for this policy and the relevant procedure, Computer Center Access & Maintenance Procedure.
- B. Information Services is responsible for developing the procedures for authorizing access to the CWUCC. (See Appendix A - Computer Center Access & Maintenance Procedure.)

## **(4) Policy Maintenance**

- A. The CIO will review and recommend changes to this policy statement at least annually or more frequently as needed to respond to changes within the institution and the regulatory environment.

### **History:**

*Responsibility: AVP of ISS; Authority: Cabinet/UPAC; Reviewed/Endorsed by: Cabinet/UPAC; Review/Effective Date: 02/11/2015; Approved by: James L. Gaudino, President*  
*Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-060, June 2025*  
*Attached Procedure CWUR 7-70-020 as Appendix A, June 2025*

## Appendix A - Computer Center Access & Maintenance Procedure

### **(1) Purpose:**

- A. This procedure supports the Computer Center Access & Maintenance policy; defines how personnel are authorized for access and defines the sign-in, sign-out process; and applies to anyone requiring access to the CWU Computer Center (CWUCC) including, but not limited to, all students, faculty, staff, student employees, and outside contractors that are affiliated or conduct work on behalf of the University.

### **(2) Authorized Access Process:**

- A. Information Services (IS) will authorize all employees and personnel that require physical access to the CWUCC according to established procedures.
- B. IS pre-authorizes access to the CWUCC which permits access without escort.
- C. Access requests must be approved by a CWU Dean or Director-level staff on behalf of the student, faculty, staff, or contracted requester.
- D. Authorized Access requests are to be sent via e-mail from the Dean or Manager level staff to the CWU Service Desk.
- E. The CWU Service Desk will forward the request to the Director of Networks & Operations (N&O) for approval.
- F. The Director of N&O will approve or deny the request. Processing and management of requests can be delegated at her/his discretion.
- G. Personnel who are granted Authorized Access will receive training for the Halon Fire Suppression system from N&O personnel.

### **(3) Permanently Assigned Employees:**

- A. Employees with clear Background Checks can be permanently assigned to a work space in the Computer Center. Permanently assigned employees are not required to sign-in and sign-out while accessing the Computer Center.

### **(4) Unauthorized Access:**

- A. Students, faculty, staff, and contractors with a business purpose to access the CWUCC who have not been pre-authorized, will be granted access and escorted by IS personnel while in the facility.
- B. Persons without a business purpose will be denied access and IS personnel will contact Campus Security as a situation warrants.

**(5) Sign-In, Sign-out Procedure:**

- A. All personnel requiring access to the CWUCC will register at the main Operations Desk.
- B. All personnel requiring access to the CWUCC who are not permanently assigned are required to register at the main Operations Desk prior to access. Individuals without prior Authorized Access will be escorted by IS personnel. Individuals will register by notifying IS personnel of their need to access the facility and by logging the following information into the CWUCC Access Log:
  - 1. Name (Full name printed);
  - 2. Signature;
  - 3. Department/Company name;
  - 4. Phone number or University extension;
  - 5. Purpose of visit/access;
  - 6. Time In/Time Out.
- C. IS staff may validate business need as the situation warrants.
- D. Personnel accessing the facility whose work/purpose has the potential to impact the operational status or integrity of the Computer Center are required to:
  - 1. Schedule the work in advance with IS N&O Staff;
  - 2. Provide IS N&O staff with a description of the work to be accomplished;
  - 3. Document the change(s) to be made;
  - 4. Coordinate work schedule with IS N&O.
- E. Areas of work which impact the operational status or integrity of the facility may include, but not be limited to:
  - 1. Network and data infrastructure changes;
  - 2. Air Conditioning and Air Handling equipment;
  - 3. Power including street, generator, battery backup and local service;
  - 4. Telecommunication Services;
  - 5. Fire Suppression;
  - 6. Plumbing and drainage.

- F. IS N&O staff are to be notified in advance for activities noted in sections 5.C and 5.D. It is not enough to simply arrive and inform the Operations staff on duty if the work has the potential to impact operational status or integrity of the systems housed in the CWUCC. Notification can be made through the IS Service Desk who will in turn notify IS N&O.

**(6) Emergency Situations:**

- A. In the event of an emergency during hours when the CWUCC is not staffed, authorized personnel requiring access may do so without prior notification.
- B. Emergency situations are limited to events which are highly likely to adversely impact the operational integrity of the CWUCC, or may result in equipment damage or injury to personnel. Personnel are to register and notify IS Operations Staff at the earliest convenience with the specifics of the emergency and actions taken.
- C. IS N&O will provide a list of emergency contacts at the CWUCC main Operations Desk near the vicinity of the Sign-In, Sign-Out Access Log.