**Access Control**

*Effective: July 2025*

### **Purpose**

The purpose of this policy is to establish guidelines for granting, managing, and revoking access to physical facilities and digital resources within Pierpont Community and Technical College (PCTC). The objective is to safeguard people, property, and data by ensuring that only authorized individuals can access specific areas and systems.

### **scope**

This policy applies to all students, faculty, staff, contractors, visitors, and any third parties who require access to community college facilities or information systems.

**1. Definitions**

* **Access Control**: The selective restriction of access to resources.
* **Physical Access**: Entry to buildings, rooms, and facilities.
* **Logical Access**: Use of information systems, including email, academic platforms, and databases.
* **Authorized User**: An individual who has been granted access rights through proper approval channels.

**2. Policy Statements**

 **2.1 Physical Access Control**

* **Building Access**:
	+ Main campus buildings are open to the public during published business hours.
	+ Access outside of business hours requires prior authorization.
* **Restricted Areas**:
	+ Labs, server rooms, and faculty offices are accessible only to authorized personnel.
	+ Electronic keycards or codes may be used to manage access.
* **Key Issuance**:
	+ Physical keys and access cards are issued through the Facilities Department.
	+ Lost keys or access cards must be reported immediately.

 **2.2 Logical Access Control**

* **Account Management**:
	+ User accounts are provisioned by the IT Department upon enrollment or hiring.
	+ Accounts are deactivated when a student graduates, withdraws, or a staff member separates.
* **Authentication**:
	+ All systems require secure authentication (e.g., unique ID and password).
	+ Two-factor authentication (2FA) is required for administrative and faculty access.
* **Role-Based Access**:
	+ Access to systems is granted based on the principle of least privilege.
	+ Academic staff, administrative personnel, and students receive access appropriate to their roles.

 **2.3 Visitor Access**

* All visitors must register at designated entry points.
* Escorts may be required for access to restricted areas.

 **2.4 Monitoring and Auditing**

* Access logs for both physical and logical systems must be maintained and periodically reviewed.
* Unauthorized access attempts will be investigated and may result in disciplinary action.

 **2.5 Revocation of Access**

* Access rights are immediately revoked upon termination of affiliation with the college.
* Temporary or expired credentials must be deactivated promptly.

 **3. Responsibilities**

* **IT Department**: Manages logical access systems, user accounts, and cybersecurity measures.
* **Facilities and Campus Security**: Oversees physical access systems and security protocols.
* **Deans and Faculty**: Approve access requests for personnel under their authority.
* **Users**: Must follow all access control guidelines and report suspicious activity.

**4. Enforcement**

Violations of this policy may lead to disciplinary action, including but not limited to suspension of access privileges, academic penalties, or employment termination.

**5. Review and Revision**

This policy will be reviewed annually by the IT and Facilities departments and revised as necessary to reflect technological, procedural, or regulatory changes.