Policy Title	**Critical Information Technology Spaces Physical Security and Access**
Policy Number	8020
Category	Technology (8000s)
Applicability	College-wide
Responsible Office	Information Technology Services
Effective Date	June 16, 2025

I. Policy Statement

Critical information technology (IT) spaces, as defined within this Policy, must be appropriately designed, and access must be appropriately controlled, to ensure these spaces remain secure and to reasonably prevent unauthorized access.

II. Rationale

To support sound College-wide information security practices and compliance with various State and Federal regulations and law, this Policy supports the Office of Information Technology Services (ITS) to safeguard and maintain the integrity, confidentiality, and availability of College services and data.

To that end, this Policy will: 1) define which members of the College have the need and authorization to access specified critical IT spaces, 2) explain how access to these spaces will be controlled, and 3) set rules governing the use of and expected conduct while accessing these spaces.

III. Scope and Applicability

This Policy governs physical security standards and access to all critical IT spaces, and applies college-wide to all administrative units, departments, employees, students, contractors, vendors, and guests of the college.

IV. Responsible Office/Executive

The Office of Information Technology Services has responsibility for the implementation and review of this Policy. Individuals with questions about this Policy should contact the Office of Information Technology Services for more information.

V. Definitions

Critical IT Space: An area containing critical IT infrastructure, including but not limited to:

- Data centers (facilities in which computer servers, network, or telecommunications equipment are housed and operated; data centers typically require and have specific

electrical, network, HVAC, and other design elements to support optimal, uninterrupted operations);
- Server rooms (smaller facilities where computer servers, network, or telecommunications equipment are housed and operated; these may also have specific electrical, network, HVAC, and other design elements to support optimal, uninterrupted operations);
- Data/remote closets (dedicated, secure closets or small rooms that house a main distribution frame (MDF), intermediate distribution frame (IDF), and/or other critical IT equipment such as servers, routers, wireless access points, switches, voice/data systems, alarm systems, or security cameras; these may also have specific electrical, network, HVAC, and other design elements to support optimal, uninterrupted operations);
- Telecommunication facilities (smaller rooms or facilities where telecommunication/network cabling is placed, connected, organized, or terminated;
- Other similar locations in which critical IT infrastructure is housed.

Access Control: a system for securing and controlling access to a critical IT space, including but not limited to card access, biometric access, specialized key control, and similar technologies.

Authorized Individual(s): College employee(s) who have authority by virtue of this Policy to independently access and to grant temporary access to a critical IT space to other College employees (Authorized Persons) or to Authorized Visitor(s), subject to the reasons and conditions outlined within this Policy.

Authorized Person(s): College employees who have received authorization from an Authorized Individual to enter and access specific critical IT space(s) for a specific purpose and period of time.

Authorized Visitor(s): College contractor/vendor or other external individual/entity who has received authorization from an Authorized Individual to enter and access specific critical IT space(s) for a specific purpose and period of time.

VI. Policy Elaboration

A. Minimum Physical Security Standards for Critical IT Spaces

Critical IT spaces require appropriate design and access control(s) to reasonably prevent physical intrusion and unauthorized access, including but not limited to:

- Safety (such as fire extinguishers and other fire safety features; adequate lighting and aisle/cabinet access; posted safety/emergency procedures; prohibition on combustible materials; signage prohibiting food, drink, unauthorized videography/photography);
- Environmental (such as HVAC and cooling systems, sufficient primary and backup power sources/supplies; water intrusion alarms; cleaning schedule);
- Security (such as external and internal locks; alarms; cameras; access monitoring; access controls and other features to reasonably prevent bypass of physical security elements);
- Organization (such as clear labeling of equipment, power sources, cabling, switches, etc.; inventory of equipment; accessible documentation)

B. Authorized Individuals

The following employees are authorized to independently access and to grant temporary access to a critical IT space to others:

- The College Administrative Director of Infrastructure Services;
- The next level administrator of Infrastructure Services; and
- In the absence of the Authorized Individuals listed above, another employee designated in writing by the Vice President for IT/Chief Information Officer.

C. Access to Critical IT Spaces

Accessing any of the College's critical IT spaces by persons without formal authorized access in accordance with this Policy is strictly prohibited. Access control to critical IT spaces requires specially configured access. Alternatively, an employee with a valid college ID, confirmed identity, and authorized purpose (Authorized Person) may be escorted to a critical IT space by an Authorized Individual.

Any individual who is permitted access to a critical IT space must exercise due caution in the physical care of the equipment housed therein. Should equipment that was not intended for service be impacted or damaged, this must be reported immediately to the College Administrative Director of Infrastructure Services.

Persons who are permitted access to a critical IT space must maintain the space in an appropriate state of cleanliness and orderliness and promptly report any incidents or concerns regarding cleanliness and orderliness.

Access to Data Center(s):

The College Administrative Director of Infrastructure Services will maintain a roster of Authorized Individuals who are permitted independent access to the Data Center. Any disputes pertaining to rejected access requests must be reported to the College Administrative Director of Infrastructure Services for determination. If there is a security issue or incident arising out of unauthorized access, the Information Security Officer will also be notified and engaged as needed. The Authorized Persons list will be reviewed by the College Administrative Director of Infrastructure Services, the Associate Director of Data Warehousing (at times alternatively referred to as the Associate Director for the Data Center) and the Information Security Officer bi-annually.

Authorized Visitor Access:

Any temporary access by an authorized visitor (non-employee, vendor) requires direct supervision by an Authorized Individual throughout the visitor's time in the data and communications distribution locations. Visitors must be tracked in a logbook, stating the purpose of their visit and equipment accessed, with signatures by the visitor and by the College escort.

Access Monitoring:

The College Administrative Director of Infrastructure Services and the Associate Director of Data Warehousing will monitor all access to critical IT spaces and will respond to unauthorized access attempts as appropriate. If installed, cameras will monitor access to critical IT spaces. Recorded camera feeds will be used as needed in any required investigations.

If unauthorized access is suspected by any individual, they must immediately notify Public Safety, who in turn will immediately notify the College Administrative Director of Infrastructure Services or Associate Director of Data Warehousing. If the incident requires a formal investigation, as determined by the College Administrative Director of Infrastructure Services, Associate Director of Data Warehousing, or the Public Safety supervisor on duty, Public Safety will then immediately notify the Information Security Officer. Potential security incidents or breaches will be addressed in accordance with the college's cybersecurity incident response plan.

Penalties and Enforcement:

Individuals who violate this policy are subject to restriction or loss of access to the college IT environment and/or computing privileges, and could be subject to civil and criminal penalties. Disciplinary sanctions will be subject to the procedures set forth in the respective collective bargaining agreements or as otherwise provided for by applicable law, regulation, or college policy. Violations of this policy by vendors or contractors may result in termination of contracts or commitments to the vendor/contractor.

VII. Related Administrative Procedures

The Vice President of Information Technology Services is authorized to develop and disseminate reasonable rules and procedures as necessary to implement this Policy.

VIII. Cross-References

- Other College policies governing technology and information security can be accessed on the Legal Affairs webpage.

IX. References

- Middle States Commission on Higher Education (MSCHE) Standard VI

X. History / Revision Dates

Adoption Date: June 16, 2025 (President's Cabinet)