Policy Title: IT Physical Security Policy	**Effective Date: 09/4/2008**
Policy ID: IT-PO-5203	**Review Date: 06/26/2026**
Oversight Executive: Associate VP for IT & CIO	**Next Review Date: 06/26/2027**

1. PURPOSE

The purpose of this policy is to establish requirements for physical facilities that house information technology equipment, systems, services, and personnel. Physical security controls prevent unauthorized access, damage or interference with university technology information and assets.

2. APPLICABILITY

This policy applies to physical facilities that house information technology equipment, university technology personnel, vendors, or visitors requiring access to these physical spaces.

3. DEFINITIONS

Least Privilege: A person is only given the minimum level of access needed to perform duties.

4. POLICY

A. Physical access to information resources is to be restricted commensurate with the classification of the resource and the level of risk.

B. Areas containing critical information resources require special safeguards that provide the appropriate levels of protection against human, natural, and environmental risks to achieve a high level of availability.

C. Mission critical systems must be located in a secure location that is restricted to authorized personnel only. Access to critical computer hardware, wiring, displays and networks must be controlled by rules of least privilege.

D. Access cards and/or keys must not be shared or loaned to others.

E. A system of monitoring and auditing for physical access to critical computer hardware, wiring, displays and networks must be implemented (e.g. card swipe and door access logs).

F. Visitor access to critical areas must be documented with a sign in / sign out log and they must be escorted at all times.

G. Rooms with restricted access must have the appropriate signage.

H. Entry logs for data centers must be reviewed on a weekly basis by the operations staff. Attempted unauthorized access will be reported to the CISO and the Director of IT Infrastructure.

I. The Data Centers' System Owner will review biannually the list of persons with card and/or key access to IT facilities.

5. PROCEDURES

Information Technology Services (ITS) has developed specific standards, procedures, and guidelines, as appropriate, for the implementation of this policy and management of the IT functions of the University. These standards, procedures, and guidelines are maintained and hosted by ITS.

6. EXCLUSIONS

None

7. APPENDICES

None

8. REFERENCES

Code of Virginia, Title 23.1, Chapter 10 (§ 23.1-1000 et seq.), "Restructured Higher Education Financial and Administrative Operations Act."

Chapter 824, Virginia Acts of Assembly 2008, "Restructured Higher Education Financial and Administrative Operations Act"

Chapter 829, Virginia Acts of Assembly 2008, "Restructured Higher Education Financial and Administrative Operations Act"

9. AUTHORITY AND INTERPRETATION

Information technology is managed under delegated operational authority granted to the University by the Virginia General Assembly, as set forth in the Restructured Higher Education Financial and Administrative Operations Act, § 23.1-1000 et seq. of the Code of Virginia, and Chapters 824 and 829, Acts of Assembly, 2008. The Board of Visitors (Board) approved the University to operate under this delegated authority in Board resolutions dated April 23, 2009, and May 4, 2012. Accordingly, the authority to interpret this policy rests with the President of the University and is generally delegated to the Vice President for Information Technology and Chief Information Officer (CIO).

10. APPROVAL AND REVISIONS

The *IT Physical Security Policy* was initially approved by the Vice President for Information Technoloyg & CIO on December 18, 2008. The policy was revised on July 28, 2008, to reflect a change to access request, signage and log entry review procedures. The policy was reviewed July 1, 2012, with no change, and updated with new university branding November 3, 2015.

The new *IT Physical Security Policy*, reformatted into the University-wide policy template, was submitted to and approved by the President's Cabinet at the meeting held on xxxxx, and was signed by President Kyle.

Reviewed: 8/5/2024

Minor wording changes.

Reviewed: 06/26/2026

Wording changes.

Approved by: CISO Bob Burton on June 26, 2026.

For general information concerning University policies, contact the Office of Policy Compliance – (540) 831-5794. For questions or guidance on a specific policy, contact the Oversight Department referenced in the policy.