NSCS Information Security Standard 9: Physical Security

In addition to the specific restrictions identified in this Standard, IT Standard 9 must comply with and inform Campus Physical Security policy and procedure.

Physical Security for the information technology infrastructure should also adhere where possible to the principle of least access.

9.1 College Data Centers

On and off-campus data centers should at minimum meet the following requirements:

- Physical access to data centers is limited to authorized Information Technology (IT) personnel, designated approved employees, IT employees of organizations with a data-center sharing agreement with the College, or contractors whose job function or responsibilities require such physical access. All others are considered visitors and access can only be approved by the CISO.
- Access shall be controlled by electronic or brass key means in compliance with Campus Physical Security Policy.
- Visitors accessing data centers will be accompanied by authorized personnel.
- Video surveillance of data centers is required.

9.2 Telecommunication Closets

The following requirements apply to telecommunication ("telecom") closets.

- Telecom closets are not to be used for storage, custodial services, or offices. Combining electrical and telecom closets with controlled access is an acceptable practice.
- Telecom closets are to be locked and access limited to only those individuals approved by the CISO.
- Telecom closets are to remain free of combustibles.

Revision History

April/14/2019:	Initial submission by PCSS
May/8/2019:	Initial review by SOISO/CISOs
July/8/2019:	Second review by SOISO/CISOs
July/26/2019:	Third review by SOISO
Oct/1/2019:	Fourth review by SOISO