NSCS Information Security Standard 8: Email

The NSCS provides employees and students with a supported email service subject to the requirements below:

Shared email accounts are allowed when approved by the CISO but should be configured with delegation rather than credential sharing.

Using personal devices for email management is permitted but must conform to Standard 15 – Bring Your Own Device (BYOD).

Email originating outside of NSCS is to be scanned for malware and checked for SPAM and phishing attacks. These filters will be adjusted at the discretion of the CIO/CISO to maximize the amount of malicious email blocked while minimizing false positives.

Employees shall not use non-NSCS email systems for NSCS business.

If high or medium risk information must be transmitted via email, then email encryption must be used.

Follow precautions regarding e-mail as recommended by IT security training.

Report malicious SPAM and phishing email within the e-mail application or to the helpdesk, and if there is a concern that an action has occurred that may have compromised security, contact the helpdesk immediately. If in doubt, call the helpdesk.

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