NSCS Information Security Standard 13: Cloud Computing

The requirements below help to ensure that NSCS data are appropriately stored or shared using Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

- Where NSCS authentication is impractical for web-based SaaS cloud services due to size or nature of service, employees must use their NSCS supported e-mail to register the account for work related cloud services and manage passwords in a NSCS provided password vault or, if none is provided, in such a way that passwords are easily recoverable by the NSCS in the event of separation or injury.
- To mitigate the risk of a data breach occurring as a result of compromised credentials (such as through a successful phishing attack), multi-factor authentication is required when accessing SaaS solutions involving High Risk data from outside of NSCS networks.
- The individual(s) responsible for managing user access levels and roles must be identified and under the direct or indirect supervision of the CISO.
- NSCS information assets stored in the cloud shall be protected with no less control than that used for on premise systems.
- Protected medium and high-risk data (including credentials) stored in the cloud (including test and development environments, backups and data warehouses) must be encrypted both at rest and in transit.
- Encryption keys must be held by NSCS unless the vendor has appropriate key management in place.
- Each College shall have a procedure for vetting cloud services to ensure data security and disaster recovery requirements are met prior to contracting.

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