NSCS Information Security Standard 6: Computer and Network Security

6.1 Endpoint Security

Endpoints with updatable operating systems, including but not limited to: servers, network devices, desktops, portable (laptops and tablets), printers, copiers, Internet-of-Things devices, and phones owned and/or managed by the NSCS or third party contractors are to be configured using the standards detailed below:

- All systems are to run vendor supported versions of operating systems approved by the CIO.
- All default accounts are to be removed or default account passwords are to be changed prior to installing a system on an NSCS network. This includes but is not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and SNMP community strings.
- Operating systems (OS's) and applications must be kept-up-date on computers and devices that access NSCS networks whether or not they process or store NSCS confidential information. Apply patches based on severity ratings such as the National Vulnerability Database (NVD), apply critical/high severity security patches within seven (7) calendar days of being published, medium severity within thirty (30) calendar days. If a legitimate business reason exists for not patching a system in compliance with this clause, a security exception can be submitted to the CISO for consideration.
- Unneeded accounts, such as guest accounts, should be deleted or disabled.
- Endpoint based firewall functionality installed where feasible.
- Hard drives within portable endpoints must be protected with encryption technology.
- Endpoints not protected by physical access controls (locked doors, etc.) must be configured to prevent unauthorized change of firmware settings.
- All standard, supported software for desktops and laptops will be administered from the Information Technology (IT) department.
- The IT department reserves the right to review and remove software which may be detrimental to the security or functionality of NSCS owned systems.
- The principle of least functionality shall be used to configure endpoints. Non-required services should be disabled.
- Set inactivity timeout of no more than 15 minutes.
- Endpoints should be configured to automatically synchronize system time with a reliable time server.

6.2 Server Security

In addition to the general endpoint security noted in Standard 6.1, the following controls will be followed for servers:

- Operating system and application updates shall be applied during routine maintenance windows as defined by campus procedure. Critical patches may be applied during emergency maintenance periods based upon the risk as determined by the CISO.
- Service processes should be configured according to the principles of least functionality and least privilege.
- Disable unencrypted services where possible.

6.3 Application (Website) Security

- Web pages that collect private information must display a link to a Privacy Statement.
- Only Low-risk information can be made publicly accessible on externally facing websites.
- If authentication mechanisms are used, ensure that they occur over HTTPS.

6.4 Anti-Malware Software

The following outlines the high-level requirements for end-point protection (EPP).

- All NSCS laptops, desktops, and servers must run NSCS issued anti-malware software.
- Anti-malware software must utilize an industry best practice method to identify malicious software and/or behavior.
- Anti-malware should be configured to report to a central console for management and for alerting.
- Anti-malware software is to be updated automatically and routinely, at minimum weekly, and immediately when an identified threat has been determined.
- If available, Anti-malware is required on mobile devices.

6.5 Firewalls, Network and Perimeter Security

- Network connectivity devices must be authorized to connect to an NSCS network with prior approval by the CISO. This includes but is not limited to routers, switches, hubs, wireless access points or any multiport device. Devices attached to the network without authorization may be removed, disconnected, or suppressed to protect the integrity of the network.
- Network devices, services, and endpoints should be configured to use the most secure protocol version which supports the business need.
- The NSCS network architecture will implement systems in protected network segments isolated from user networks and the internet.
- All site-to-site layer 2 and layer 3 (VPN) connections from an NSCS internal networks to external networks must be approved and managed by the CISO. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures in place.

- Network device management access will be protected and controlled through the use of the following control enhancements:
    - Admin accounts will rely on single-sign-on methodologies where available. Non-integrated admin accounts will be password protected and meet NSCS Admin (privileged) account complexity requirements.
    - Local password storage will be encrypted.
    - Admin accounts will be limited and carefully controlled.
    - Traffic that can terminate on the device itself must be limited to legitimate use.
    - Console and auxiliary port access will be password protected.
    - Physical access to the device will be protected where possible.
    - The Login Password Retry Lockout feature will be set to five or less.
    - Session Timeout will be set to fifteen (15) minutes or less.
    - Each router must have a login banner indicating that misuse is prohibited.

- Unnecessary networking protocols and services on perimeter control devices will be disabled or not allowed.
- Configuration of Network Time Protocol (NTP) is required where available.
- The following defines the minimum configuration requirements for NSCS firewalls.
    - Exceptions to perimeter security controls must be documented with a business need, a specified duration of that need, and approved by the CISO.
    - Where possible, the NSCS preference is to install a hardware-based firewall as a network perimeter security control.
    - All Internet traffic from inside to outside, and vice-versa, must pass through an NSCS managed firewall.
    - Tools should be in place either at the NSCS firewall level or through the internet provider to prevent and/or manage distributed denial of service attacks.
    - Perimeter firewall architecture implements a managed access policy for each external service.
    - Firewall implementations will use application proxy or stateful aware technologies where applicable.
    - Firewall and network boundary interfaces shall deny inbound (ingress) network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Inbound permit rules shall be reviewed periodically.
    - Drop incoming packets at the device sourced with invalid addresses, such as internal or RFC1918 addresses arriving on an external interface.
    - Firewall technology may be used to block access to sites that may pose a threat to NSCS networks.

6.6 VPN Access Connections

Virtual Private Network (VPN) connections to NSCS resources are an extension of the NSCS network and subject to NSCS's policies. VPN connections to the NSCS network must meet the following requirements:

- A user's remote access to NSCS resources is allowed only with the use of CISO approved methods.
- Remote devices connected to an NSCS network will be configured so that all data traffic uses the VPN connection (no split-tunneling).
- Connections are automatically ended after thirty (30) minutes of inactivity for service and security reasons.

6.7 Wireless Networks

All wireless infrastructure devices that connect to an NSCS network or reside in a NSCS office must adhere to the following guidelines:

- Use 802.1x authentication where available for wireless connections to the network.
- Where 802.1x authentication is not available, devices must be registered with the wireless management system.

6.8 Vulnerability Testing

The following requirements apply to vulnerability scanning and the associated tools.

- The use of tools to test the vulnerability of IT resources is limited to authorized personnel.
- Vulnerability testing must be coordinated with the owner of the impacted IT resources.
- Vulnerability testing is required on a regular basis, quarterly is preferred.
- Critical and high severity items identified in vulnerability scans must be addressed according to schedules provided in section 6.1 Endpoint Security, and followed by a retest, repeating these steps until the vulnerability testing completes successfully.
- External and internal vulnerability testing shall be performed after any significant infrastructure or application change.
- Vulnerability testing shall minimally consist of network-layer and application-layer penetration test.

6.9 Auditing and Activity Monitoring

The NSCS recognizes that auditing and activity monitoring is a very resource intensive function. Each College shall have a systems list with priorities determined by the CISO and plan for implementation of this Standard (6.9) on a per system basis as resources allow. Colleges will use the auditing capabilities within available systems to monitor both authorized and unauthorized activities, with the focus on unauthorized or malicious activities:

- Audit and activity monitoring should include the details associated with authorized access, privileged operations, unauthorized access attempts, system alerts or failures, and changes or attempts to change system or security settings.
- Audit logs are to be maintained a minimum of one month, preferably six months.
- Audit logs may store sensitive information and should be protected from unauthorized access.
- Where the staffing levels allow alternate staff assigned to review logs for suspicious activity to ensure that multiple people are reviewing the logs including the logs for each other.
- The CISO is ultimately responsible for determining when action is required to address anomalous activity.
- Where possible, log analysis should be automated, combined with event correlation software and continually improved to detect current threats to NSCS networks, information assets, anomalous behavior, abuse or misuse of resources.
- Logs should be sent to a log server configured to prevent and detect tampering attempts to log records or files.
- It is imperative that system time is synchronized across information systems within NSCS information processing facilities to enable the accurate detection of event and correlation of activities across information systems and for the legal admissibility of evidence.
- Administrator and operator logs should be monitored on a regular basis as staffing levels permit for unauthorized access and anomalous behavior.

6.10 Third Party Technology Contractor Information Systems Access

- All remote vendor support must be performed using auditable encrypted sessions with appropriately secure ciphers.
- Once VPN is authenticated, remote support may be accomplished via virtual console, remote desktop, or similar tool as determined by platform and business need.
- The vendor will have a dedicated account (or accounts) with access limited to facilitate only the business functions required under the service agreement.
- Upon termination of the support engagement, NSCS staff must:
    - Ensure remote session has been terminated.
    - Disable the vendor support account.

6.11 Computing in Public Areas

Computer systems and infrastructure within public places require additional controls including:

- Open ports in public areas are to be disabled until needed or utilize access control and provide only Internet access to guest users.
- Kiosks are to require log-on credentials unless the system is configured to only access the Internet.

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