NSCS Information Security Standard 15: Bring Your Own Device (BYOD)

Use of NSCS networks in conjunction with personal devices for non-work related functions by members of the NSCS community is governed by Standard 5: Acceptable Use Policy (AUP). This Standard (15) provides guidance for employee use of personal devices for work related functions beyond the guidelines indicated in the AUP.

NSCS grants its employees the convenience of using personal devices provided that the device meets the security and compatibility requirements of the College or the System Office. The NSCS reserves the right to revoke this privilege if users do not abide by NSCS policies and procedures.

This Standard is intended to protect the security and integrity of NSCS Technology Resources.

NSCS employees must agree to the terms and conditions set forth in this Standard and the Acceptable Use Policy in order to be able to use their personal device for work related functions.

Device Protection and Support

- Mobile devices connected to the campus wireless networks must follow device registration procedures established by the college;

- Mobile device connectivity to the campus wireless networks and troubleshooting are supported by the IT departments on a best effort basis only. Support is not provided for home based computers;

- Devices used to access technology resources must at a minimum:
  Run a supported version of the operating system
  Run a current version of anti-malware and execute scheduled device scans
  Use Password protection features of the device
  Auto-lock when not in use

- Devices used to access technology resources should employ the following in order to further prevent unauthorized access:
  Device encryption

- The NSCS reserves the right to disconnect devices or disable access to services without notification.

Responsibilities

- Employees are not permitted to download or store data considered to be sensitive on personal devices. Sensitive data is defined as High or Medium Risk as indicated in Standard 4. Questions regarding the category of data should be referred to the Chief Information Officer.

- It is the employee's responsibility to ensure that NSCS data and applications are removed from a device in the event that the employee is separated from employment, or if IT detects a data or

policy breach, a virus or similar threat to the security of the NSCS's data and technology infrastructure.

- In the event a device is lost or stolen, it is the employee's responsibility to use provider tools, where available, to remotely wipe the device of all data. Lost or stolen devices should be reported to the Chief Information Officer within 24 hours in order to assess risk to technology resources and to advise the employee accordingly.

- It is the employee's responsibility to back up email, contacts, and any other important data on the device.

- The employee is personally liable for all costs associated with his or her device.

- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of NSCS and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

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
Sept/30/2019:	Fourth review by SOISO/CISOs using campus feedback