Policy #12.5
Date Approved:
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: MOBILE DEVICE POLICY

1.0 PURPOSE

Snow College is committed to and encourages an open and collaborative environment through the use of mobile devices to facilitate academic interaction among students, faculty and staff. There is an inherent risk in utilizing mobile devices for this purpose.

The purpose of this policy is to clearly state the college policy and user requirements necessary to mitigate this risk and to protect the college or Personally Identifiable Information (PII) stored on mobile devices.

2.0 POLICY

It is the responsibility of anyone who utilizes the Snow College internal network for the purpose of accessing or processing College PII using a mobile device to take appropriate measures at all times to safeguard that information.

All such individuals ("Users") will ensure they are taking every reasonable precaution against accidental or intentional data compromise by implementing the measures prescribed in Appendix A of this policy for their mobile devices.

3.0 DEFINITIONS

3.1. *Mobile Device.* Any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

3.2. *Personally Identifiable Information (PII)*. Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are credit card and social security numbers

3.3. *Personal Identification Number (PIN).* This can be any combination of numbers (usually a minimum of four (4)) that is used to unlock a device.

3.4. *Encryption*. The use of software or hardware to make data unreadable unless the device is presented with the correct password or PIN. Most mobile devices include this feature but require the user to enable it.

3.5. *Remote Wipe*. The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

3.6. *Malicious Software*. Often called malware, this is software designed to disrupt computer operation, gather PII, or gain unauthorized access to computer systems.

3.7. *Anti-virus Software*. Software designed to detect and/or remove malicious software and viruses from a computer system.

3.8. *Data Security Steward*. Individuals within the different College organizations, appointed by the division dean who are points of contact for security violations or issues and act as a general reference within their work centers for information security topics.

3.9. *Strong Password*. A password that is at least eight (8) characters long and is a combination of upper and lower case letters, numbers and special characters. Strong passwords do not include phrases, names, or other types of dictionary words.

3.10. *Security Patch*. A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most mobile devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

4.0 REFERENCES

Understanding and Identifying PII, Internal and Public Information

12.1 Information Technology Acceptable Use Policy

12.2 Data Classification and Handling Policy

12.4 Information Security Policy

Appendix A - Standards

- No mobile device shall be used to store PII unless the user complies with 12.4 Information Security Policy.
- All use of mobile devices, **College or personally owned**, which utilize College network resources, will be subject to the provisions of 12.1 Information Technology Acceptable Use Policy.
- All mobile devices will be kept up to date with the latest possible operating system, security patches, and application versions.
- All applications (apps) will be updated with the latest security patches.
- All devices will be configured with a PIN, pattern, or password-enabled lock screen configured to activate at no more than 5 minutes of inactivity.
- All devices with built in Encryption capability will have onboard Encryption enabled.
- All devices will have Remote Wipe enabled either through Mobile Sync, a third party app or the manufacturer's website.
- All devices that have been used to store, access and/or process PII will be wiped and overwritten to remove such data before they are transferred to someone else through sale or gifting.
- In the event that a device which has been used to store, access and/or process PII becomes lost, stolen or compromised, the owner must comply with the reporting requirements of 12.4, Information Security Policy. For a listing of the data security stewards by division, please refer to the data security stewards document maintained by the Information Security Office. Additionally, in case of loss, the user must immediately contact the IT service desk to request remote wiping through mobile sync if that service is utilized on the device. Otherwise, the user will request mobile wiping through the device's manufacturer.