Policy Name	Mobile Device Security Policy
Policy Number	50000.007
Effective Date	January 25, 2016
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	February 13,2019

1. Policy Statement

Mobile devices represent a significant risk to information security and data security if the appropriate security applications and procedures are not applied, they can be conduits for unauthorized access to the University's data and IT infrastructure. This can subsequently lead to data leakage and system infection. JSU has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Definitions

2.1. Information Technology ("IT") - use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
2.2. Mobile Device - a portable computing device such as a smartphone or tablet computer.
2.3. Mobile Security - the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.
2.4. Jailbroken device - a mobile device that has had the limitations imposed by the manufacturer removed. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

3. Employee Adherence

University employees and students who use a laptop computer or mobile device (e.g. portable hard drives, USB flash drives, smartphones, tablets), not including University IT-managed laptops) are responsible for the University data stored, processed or transmitted via that computer or mobile device and for following the security requirements set forth in this policy and other applicable IT Security Policies and regulations regardless of whether that device is the property of the University or the individual.

4. Policy

4.1. **Technical Requirements**

4.1.1. All mobile devices must use the latest operating systems provided.
4.1.2. If users are saving passwords on devices, they must be encrypted through the use of a password manager/vault or the use of a locked feature mechanism. (e.g., a locked note or Dashlane app)
4.1.3. JSU owned devices must be configured with a secure password that complies with JSU's password policy. This password must not be the same as any other credentials used within the organization.
4.1.4. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal University network.

4.2. **User Requirements**

4.2.1. Users must only load data essential to their role onto their mobile device(s).
4.2.2. Users must report all lost or stolen devices to JSU DIT immediately.

4.2.3. If a user suspects that unauthorized access to University data has taken place via a mobile device the user must report it to JSU DIT immediately in compliance with the University's incident handling process.

4.2.4. Devices must not be "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

4.2.5. Users must not load pirated software or illegal content onto their devices.

4.2.6. Devices must be kept up to date with manufacturer or network provided security patches through software and firmware updates. (Example: Apple iOS updates and Verizon network updates)

4.2.7. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with IT policy that outlines the device specification requirements for the University.

4.2.8. Devices must be encrypted in line with JSU's compliance standards.

4.2.9. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that University data is only sent through the University email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify JSU DIT immediately.

4.2.10. Users must not use University workstations to backup or synchronise device content such as media files unless such content is required for legitimate University and educational purposes.

5. Policy Compliance

5.1 Any user found in violation of this policy is subject to network access revoked for a limited amount of time until security training is verified by DIT.

5.2 A JSU employee's access to mobile devices purchased by JSU will be revoked and any JSU mobile device in their possession will be removed if additional policy violations occur.

6. Related Standards, Policies, and Processes

-

7. Revision History

- Policy Created: January 25, 2016
- Revised: March 7, 2017
- Revised: February 13, 2019