Policy Name	Bring Your Own Device (BYOD) Policy
Policy Number	50000.009
Effective Date	February 2, 2016
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	March 19, 2020

1. Policy Statement
   Jackson State University (JSU) grants its employees the privilege of purchasing smartphones and tablets of their choosing for work-related use. JSU reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

2. Purpose
   This policy is intended to protect the security and integrity of JSU's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

3. Definitions
   3.1 Acceptable Use is defined as use for activities that directly or indirectly support the business of JSU.

   3.2 Personal Use is defined as a reasonable and limited amount of University time spent on personal communication for recreation, such as reading or playing a game.

4. Employee Adherence
   JSU employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the JSU network.

5. Policy
   5.1. Acceptable Use
   5.1.1 Employees are blocked from accessing certain websites during work hours while connected to the University network.
   5.1.2 Employees may use their mobile device to access the following University-owned resources: email, calendars, contacts, documents, etc.
   5.1.3 Devices' camera and/or video capabilities are not disabled while on-site.
   5.1.4 Limited amount of personal apps and game apps usage are permitted during work hours.
   5.1.5 Devices may not be used at any time to:
   5.1.5.1 Store or transmit illicit materials
   5.1.5.2 Store or transmit proprietary information belonging to another university
   5.1.5.3 Harass others
   5.1.5.4 Engage in outside business activities

6. Policy Compliance
   6.1 An employee found in violation of this policy may be subject to disciplinary action and network access be revoked for a limited amount of time until security training is verified by JSU's Division of Information Technology (DIT) department.

   6.2 An employee found in repeat violation of this policy may be permanently revoked from JSU network access.

7. Related Standards, Policies, and Processes
    - Mobile Device Security, DIT-007
    - Email, DIT-001
    - Data Classification, DIT-005
    - Data Security, DIT-004
    - Data Security Definitions, DIT-001
    - Acceptable Use, DIT-003

8. Revision History
    - Policy Created: January 25, 2016
    - Document Revised: February 2, 2016
    - Document Revised: February 13, 2019