Policy 834

CISO Approval 02/09/2015

Faculty Approval 02/09/2015

**Governors State University**

**University Park, IL**

**Bring Your Own Device Policy (BYOD)**

**Effective 04/01/2015**

1. **Policy statement**
   1. **In an effort to uphold its mission to deliver an exception and accessible education experience, Governors State University (GSU) is implementing a BYOD policy for all eligible employees. It is due to the recommendations from faculty and staff that GSU resources need to be made accessible and streamlined for ease of use and access. This policy outlines the acceptable use, eligibility and enrollment, security, and support of devices.**
   2. **Access to GSU resources outline herein are: Wireless Network Access, VPN, App Library, Email, Contacts, and Calendars. Access is granted through enrollment in our Mobile Device Management System (MDM)**
2. **Acceptable Use**
   1. **GSU defines acceptable business use as activities conducted for the advancement of GSU and the advancement of higher education.**
   2. **GSU defines acceptable personal use on company time as reasonable and limited to texting, reading, and other recreational purposes.**
   3. **Usage of the WiFi network will be subject blocked sites as per employees’ personal web-access filter policy.**
   4. **Strictly prohibited device usage includes:**
      1. **Storage and transmission of illegal materials**
      2. **Harassment**
      3. **Engagement in other business activities**
      4. **Any attempt to circumvent security policies to gain access to restricted materials or unauthorized content**
      5. **Usage of GSU resources or business related activities while operating a vehicle**
         1. **Wireless headsets are recommended and will be supplied by the cost of the user**
   5. **The usage of applications will not be monitored; An ‘App Library’, hosted by GSU, will be installed after enrollment in our MDM system. Applications that can be used to access GSU data, blackboard, internal personal messaging, and other staff resources will be available for you to install on your device.**
3. **Eligibility and Enrollment**
   1. **Any eligible employee who is eligible for the BYOD policy will be required to sign the BYOD policy.** 
      1. **Completion will result in an invitation to enroll in our MDM system via text message.**
   2. **All full-time status employees are eligible**
   3. **Part-time status employees who can demonstrate a need for access may submit a BYOD access request form to their managers for approval.**
   4. **Graphical enrollment instructions are available upon request; the process is automated screen by screen requiring only the use of your personal credentials when prompted.**
   5. **GSU reserves the right to revoke the use of resources via the MDM for any reason at any time.**
   6. **Abuse of any part of the policy herein may lead to disciplinary action including, but not limited to, termination.**
   7. **VPN eligibility only available to technical staff**
   8. **One device per employee is permitted. Additional devices will require a one-time $50 license fee.**
4. **Security**
   1. **All security measure will be controlled through the MDM**
   2. **Security conditions of enrollment include:** 
      1. **Enforcement of password or unlock policy on device**
      2. **Password policies will be enforced by the MDM, which will be named device administrator, and will not be adjustable until unenrolled**
      3. **List of applications installed will be made available to the administrator**
      4. **Rooted or jailbroken devices will fail a compliance check at enrollment**
         1. **Detection of device state will be monitored and automatically unenrolled if compliances is compromised**
   3. **WiFi access is based upon the 802.1x protocol. Users will pass their GSU ID and password and are subject to the same access through admin network workstations. Likewise, exchange mail access will prompt for your credentials and the settings profile will be passed to the device.**
   4. **GSU reserves the right to remotely sanitize the device of all company data and settings for lost or stolen devices, terminations of employment, or any threats such as viruses and malware infections.**
   5. **Multiple failed password attempts will result in device lockdown. Contact administrator for assistance.**
5. **Supported devices**
   1. **Operating Systems include Apple iOS v6.0 or later, Android v3.0 or later, Blackberry, Windows Phone, Windows 7or later, Mac OSX, Chromebook, Kindle, Amazon Fire.**
   2. **Capabilities of resource support by the MDM for certain device OS will vary.**
   3. **Cell phones, tablets, PDAs, laptops, readers, netbooks, etc. are all permissible devices.**
6. **Risks, Liabilities, and Disclaimers**
   1. **Thorough attempts at creating a secure platform for access to GSU resources have been taken; however, it is the employee’s responsibility to ensure that additional precautions are taken including backups and remote device location service.**
   2. **GSU reserves the right to terminate access to any and all resources at any time for any reason without notice**
   3. **Lost and stolen devices must be reported immediately. It is the employees responsibility to contact their service provider**
   4. **Noncompliance and policy abuse may lead to termination or other disciplinary actions**
   5. **Any conditions of the device that lead to poor performance, viruses, glitches, bugs, crashes, malware, or other failures or errors that render the device unusable are fully liable to the employee**
   6. **All costs associated to the device operation and ownership are assumed by the employee**