GEORGIA SOUTHERN
UNIVERSITY

Utilization of Personal Devices (BYOD)

Area: Information Technology	Number:
Subject: Utilization of Personal Devices (BYOD)	Issued: 6/2/2014
Applies To: USG Employees	Revised:
Sources: ITS, USG IT Handbook	Reviewed:
Responsible Party: Vice President for Information Technology	Page(s): 3

I. Background and Purpose

Bring your own device (BYOD) is a concept in which members of the University community utilize their personal equipment to conduct University business. Though not unlike using home-based devices such as a personal computer or laptop to access USG data, the utilization of a device routinely brought to work poses additional risks. As such, the University System of Georgia has published a standard for BYOD in Chapter 8 of the USG IT Handbook. This standard intends to encourage the use of personally-owned devices while protecting confidential and sensitive data from unauthorized access. A BYOD security breach could result in loss of information, damage to critical applications, financial loss, and damage to the USG's public image. *Therefore, all users employing a personally-owned device connected to a University network, and/or capable of backing up, storing, or otherwise accessing sensitive data, must adhere to University and USG-defined policies, standards, and processes.*

II. Policy

The USG IT Handbook standard for BYOD and this University policy pertains to devices that employees have acquired for personal use, but also wish to use in the business environment for accessing confidential or sensitive data. It includes any personally-owned device capable of inputting, processing, storing, and outputting of USG data and connecting to a network.

Georgia Southern University encourages the use of personal devices by employees for accessing University resources insofar that users comply with the University's Appropriate Use Policy, and Requirements of BYOD users.

A. Prior Approval

BYOD users are subject to compliance with the University's Appropriate Use Policy (AUP). This policy establishes that responsibility is not based on what equipment or device is used to access the system. Rather, individuals are responsible for protecting data regardless of what form it takes or device it is on.

In this context, users who are authorized to access data are authorized to use BYOD devices insofar as they comply with the AUP and this policy.

Specifically, pertinent paragraphs of section 2 of the AUP state:

> 2b. Users must take appropriate steps to secure protected, confidential and sensitive information including personally identifying information such as social security numbers and birth dates.
>
> 2d. Only authorized devices shall be connected to the University network and no device shall be connected to the University's network or otherwise used in a manner that interferes with the authorized use of university resources. The University reserves the right to restrict the use of any technologies that may endanger the security, integrity or fair use of its information technology resources.
>
> 2f. All mobile devices that utilize campus network resources must have antivirus/anti-malware software that utilizes current virus definition files. This includes all University owned mobile devices and all mobile devices owned by faculty, students and staff that are used on the campus networks.

B. Additional Requirements of BYOD users

1. In addition, the following requirements apply to employees who BYOD and access sensitive or confidential information.

a) Utilize encryption on devices.
b) Utilize a pin, password or other secure method for accessing the device.
c) Maintain Antivirus/malware on the device.
d) Inform IT Services immediately if your device is lost or stolen.
e) Utilize only official University services for storing sensitive or confidential data.
f) Annually complete the security awareness training required by the University.
g) Backup your personal information and utilize an ITS provided utility for conducting emergency wipe-downs or lock-out of your device.

Your use of BYOD devices to access sensitive and confidential University data implies your compliance with these required practices. Visit the ITS website at http://its.georgiasouthern.edu for additional information, downloads and support.

2. The University is not obligated to support, service, repair, or otherwise make compatible any personally owned device.

a) Employees are permitted, subject to license restrictions, to install software owned by the University onto a personally owned device. Software must be removed upon termination of employment, if rights are revoked, or upon request of a supervisor, or the CIO.

C. University Owned Devices

University owned devices including, but not limited to, smart phones, tablets, and laptops that are issued or loaned to employees are also subject to the provisions of this policy.

D. Non-Compliance

If an employee who wishes to BYOD does not comply with these required practices they may be subject to enforcements associated with University/USG policy, and State or Federal Laws. Under University policy, the institution could take actions including but not limited to termination of employment, and/or seek remuneration for associated financial damages. Issues of non-compliance must be reported promptly to the Vice President for Information Technology.

III. Definitions

Confidential Data: Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Sensitive Data: Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the participant organization. Example: personally identifiable information, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA) data, or data exempt from the Georgia Open Records Act.