UNIVERSITY of West Georgia

UWG PROCEDURE NUMBER: 8.5.1
SUBJECT: UWG POLICY NAME: Bring Your Own Device ("BYOD") Policy

The Chief Information Officer, pursuant to the authority of UWG Policy 8.5.1, establishes the following procedures for compliance with the Bring Your Own Device ("BYOD") Policy:

A. Definitions.

1. ***At-Rest Files*** –computer files that may be used occasionally as reference, but are rarely or never updated. They may reside on servers, in backup storage or on the user's own hard disk.
2. ***Bring Your Own Device (BYOD)*** - Program that allows employees to use their own personal device to work, whether laptop, smartphone, or tablet, in order to interface to the internal/participant organization's network resources.
3. ***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.
4. ***Equivalent Measures*** – Data security methods that are not listed in these Procedures, but are nonetheless approved by the University Chief Information Officer.
5. ***In-Transit Data*** - Data on the move from one secure location to another, i.e., data moving from point A to point B.
6. ***Institutional Review Board*** (***IRB***) – A federally mandated body responsible for the protection of human subjects involved in research; IRB reviews, approves, and monitors research conducted by UWG faculty, students, and staff.
7. ***Mobile Device Management*** – Applications or software designed to restrict access to data stored on the device.
8. ***Personally Identifiable Information*** - Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information.
9. ***Public Data*** - Data elements that have no access restrictions and are available to the general public.
10. ***Prior-approved Devices*** – Any personal device that has been approved by the University under its BYOD program.
11. ***Sensitive Data*** - Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration, or destruction will cause potential 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.
12. ***Stored*** - Data held or at-rest, either locally or in the cloud.
13. ***Transition Period*** - A period of time whereby an object is moving from one state or level to another.
14. ***University-Owned Data*** – Any data that is created, received, or maintained by the University in the ordinary course of business. This definition does not include data created by students, unless the student is acting on behalf of the University as a student worker or intern. Students engaged in research that utilizes University data should refer and adhere to IRB requirements.

15. ***USG BYOD Standard*** – University System of Georgia IT Handbook, Section 8.0 – www.usg.edu/information_technology_handbook
16. ***University Units*** - Any institutional department or office that reports through the chain-of-authority to the University President, including divisions, colleges, schools, departments, and offices. For the sake of this Procedure, committees and task forces may be considered university units if they are operating in accordance with their charters, approved by a division vice-president.

B. Prior Approval.

Employees using personally-owned devices, software, or related components to access USG data will ensure such devices employ a method of device access protection including, but not limited to, passcode, facial recognition, card swipe, etc. University units shall establish consistent, documented, and repeatable processes that are consistent with this prior approval standard and can be considered auditable. Information Technology Services will assist and support only to the extent of providing software or applications have been purchased by the University.

C. Security.

1. Employees using Prior-approved Devices and related software shall make every attempt to keep these devices and related software protected.
2. Sensitive and Confidential Data may not be stored on a personally-owned mobile device or a Prior-Approved Device.
3. Passwords must be stored encrypted on mobile devices.
4. Backups of Prior-Approved Devices must be encrypted.
5. Employees using Prior-approved Devices and related software accessing Sensitive Data will, in addition to device access protection, ensure that the Sensitive Data is protected using data encryption while in-transit.
6. Determination of Equivalent Measures is reserved to the USG Chief Information Security Officer (CISO).
7. Managers will implement a documented process by which employees acknowledge and confirm to abide by this Procedure, as well as have all university-owned data permanently erased from their personally-owned or Prior-Approved Devices once their use is no longer required, or upon termination/resignation from employment.
8. Employees agree to and accept that their access to USG or University networks may be monitored in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.
9. Employees will immediately report to their immediate supervisor any incident or suspected incidents of unauthorized data access, data or device loss, and/or disclosure of system or participant organization resources as it relates to personally-owned devices.
10. Supervisors will immediately report such incidents to the USG CISO or UWG's Chief Information Officer.
11. Neither Sensitive Data nor Confidential Data may be stored on external cloud-based personal accounts.

D. Device and Application Support

Personally-owned Devices and software are not eligible for maintenance support from USG or UWG departments. Employees will make no modifications to personally-owned hardware or software that circumvents established USG security protocols in a significant way.

E. Non-Compliance

Failure to comply with these procedures or the USG BYOD Standard may, at the full discretion of the University, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.

Issued by the Chief Information Officer, the** 19 **day of** Sept**, 2014.

Signature, Chief Information Officer

Reviewed by President:

Previous version dated: N/A