Policy Statement

The purpose of this policy is to make users aware of South Georgia State College’s Bring Your Own Device method. SGSC will follow the guidelines established by the University System of Georgia (USG) Information Technology Handbook Section 8.0 Bring Your Own Device (BYOD) Standard.

Employees will be expected to review and acknowledge this policy during the Onboarding process in Human Resources at SGSC.

This policy applies to all SGSC employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties.

Standard

This policy will establish the process that SGSC employees must complete if they wish to perform work for SGSC on their personally-owned device.

Employees will review and complete their acknowledgment of the BYOD Policy through a course in SGSC’s Learning Management System. This course will cover the responsibilities of the employee if they choose to access, store, back up or relocate any USG or SGSC data to a personally-owned device. This course will also cover the rights of USG and SGSC, which include the right to allow or not allow this privilege. Employees will be expected to review and acknowledge this information annually through the institution’s Learning Management System.

Employees will not be allowed to connect a personally-owned device to SGSC’s “hard-wire” network.

Failure to comply with this BYOD Policy may, at the full discretion of SGSC, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.
Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
</table>
Introduction

This section establishes the standards and procedures for end users who are connecting a personally-owned device to a University System of Georgia (USG) network for business purposes.

Definitions

The following definitions of At Rest, Bring Your Own Device (BYOD), Compliance Date, Confidential Data, In Transit, Public Data, Prior Approval, Sensitive Data, Stored and Transition Period are used throughout this section.

1. **At Rest**: Computer files that are used as reference, but are not often, if at all, updated. They may reside on servers, in backup storage or on the user's own hard disk.

2. **Bring Your Own Device (BYOD)**: Refers to employees taking their own personal device to work in order to interface to the participant organization's network resources.

3. **Compliance Date**: The date by which the participant organization is expected to comply with the policy or standard.

4. **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.

5. **In Transit**: Data on the move from origin to destination.

6. **Public Data**: Data elements that have no access restrictions and are available to the general public. Also can be designated as unrestricted data.

7. **Prior Approval**: A process by which all users must gain approval prior to working with, utilizing, or implementing a process or procedure.

8. **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.

9. **Stored**: Data held or at rest, either locally or in the cloud.

10. **Transition Period**: A period of time whereby an object moves from one state or level to another.

Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
<th>Revision Date(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Purpose</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>Applicability</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td>January 2014</td>
</tr>
<tr>
<td>8.3</td>
<td>Standards</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>8.4</td>
<td>Standard Non-Compliance</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>Section Number</td>
<td>Section Name</td>
<td>Compilation Date</td>
<td>Published Date</td>
<td>Compliance Date</td>
<td>Revision Date(s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>8.5</td>
<td>Appendix A: Employee Declaration</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
</tbody>
</table>
The purpose of this standard is to empower USG staff to innovate and work on USG business more effectively inside and outside the office. Based on research at other enterprises, greater productivity and employee satisfaction should result from establishing a prudent BYOD standard that empowers employees to work on personally-owned devices while protecting the confidentiality, integrity, and availability of USG data.

This standard intends to balance the use of personally-owned devices while preventing USG data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unauthorized resources. Such a 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 USG network, and/or capable of backing up, storing, or otherwise accessing USG data of any type, must adhere to USG-defined policies, standards, and processes.
Applicability

This standard applies to all USG employees, including full- and part-time staff, consultants and other agents who use a personally-owned device to access, store, back up or relocate any USG or client-specific data. Such access to these data is a privilege, not a right, and forms the basis of a trust the USG has built with its clients, vendor partners and other constituents. Consequently, USG employment does not automatically guarantee the initial or ongoing ability to use these devices to gain access to USG networks and information.

This standard applies to any hardware and related software that is not owned or supplied by the USG, but could be used to access USG resources. This includes devices that employees have acquired for personal use, but also wish to use in the business environment. It includes any personally-owned device capable of inputting, processing, storing and outputting USG data.

This standard is complementary to any previously implemented policies and standards covering acceptable use, data access, data storage, data movement and processing, and connectivity of devices to any element of the enterprise network. Always consult the USG IT Handbook for up-to-date standards and guidance.
Standards

Section 8.3

Prior Approval

1. Employees using personally-owned devices, software, and/or related components to access USG data will ensure such devices employ some sort of device access protection such as, but not limited to, passcode, facial recognition, card swipe, etc. Within the USO, this approval authority is delegated to the first vice chancellor or above in the employee’s chain of command in consultation with the USG vice chancellor and chief information officer (VC/CIO). Participant organizations will establish and document local policies consistent with this prior approval standard.

2. Participant organizations will establish consistent, documented, and repeatable processes that are consistent with this prior approval standard and can be considered auditable.

Security

1. Employees using prior-approved personally-owned devices and related software shall make every attempt to keep these devices and related software protected.

2. Employees using prior-approved personally-owned devices and related software accessing sensitive data will, in addition to device access protection, ensure that the sensitive data is protected using data encryption or USG-provided mobile device management, or the equivalent.

3. Determination of equivalent measures is reserved to the USG Chief Information Security Officer (CISO), the information security officers (ISOs) of the participant organizations, and/or other delegated designees. Participant organizations will need to document evidence of compliance.

4. Passwords and/or other sensitive data will not be stored unencrypted on mobile devices.

5. Managers will implement a documented process by which employees acknowledge and confirm to have all USG-sensitive data permanently erased from their personally-owned devices once their use is no longer required, as defined in Section 8.2.

6. Employees agree to and accept that their access to USG 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.

7. Employees will immediately report to their managers 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.

8. Managers will immediately report such incidents to the USG CISO or the participant organization ISO as appropriate.
USG Intellectual Property 8.3.3

1. The principal storage location of state-owned data is a state-owned or contracted resource.
2. Sensitive state-owned data may not be stored on external cloud-based personal accounts.

Device and Application Support 8.3.4

1. Personally-owned devices and software are not eligible for support from USG departments.
2. Employees will make no modifications to personally-owned hardware or software that circumvents established USG security protocols in a significant way; e.g., replacing or overriding the operating system or “jail-breaking.”
Standard Non-Compliance

Failure to comply with the USG BYOD Standard may, at the full discretion of the participant organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.
Appendix A: Employee Declaration

I, ________________________, have read and understand the USG BYOD Standard and any augmenting participant organizational standards, and consent to adhere to the standards and procedures outlined therein. I, [              ] approve of the use of personal devices by this employee.

_________________________________________  ____________________________
Employee Signature  Date

_________________________________________  ____________________________
Supervisor Signature  Date

_________________________________________  ____________________________
Approval Authority Signature  Date