University System of Georgia
Creating A More Educated Georgia

Search the handbook

Go

Section 8.0: Bring Your Own Device (BYOD) Standard

Table of Contents

Information Technology Handbook

Search the handbook
Go

- Overview
- Introduction
- Section 1: Information Technology (IT) Governance
- Section 2: Project and Service Administration
- Section 3: IT Management
- Section 4: Financial and Human Resource Management
- Section 5: Information Security
- Section 6: Risk Management
- Section 7: Facilities
- **Section 8.0: Bring Your Own Device (BYOD) Standard**
- Updates and Revisions

Section 8 Introduction

Print friendly Email or share Version date October 17, 2013

This section establishes the standards and procedures for end users who are connecting a **personally-owned device** to a University System of Georgia (USG), which includes the 31 institutions, the University System Office (USO) [which includes the Shared Services Center (SSC)], the Georgia Public Library System (GPLS), and the Georgia Archives, 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 updated, if at all. 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, whether laptop, smartphone, or tablet, in order to interface to the internal/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, i.e.: data moving from point A to point B.
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 and another.

Implementation and Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date	Revision Date(s)
8.1	Purpose	October 2013	October 2013	October 2014	
8.2	Applicability	October 2013	October 2013	October 2014	
8.3	Standards	October 2013	October 2013	October 2014	
8.4	Standard Non-Compliance	October 2013	October 2013	October 2014	
8.5	Appendix A: Employee Declaration	October 2013	October 2013	October 2014	

270 Washington Street, S.W.,
Atlanta, GA 30334
U.S.A.

Information Technology Handbook

Search the handbook

Go

- Overview
- Introduction
- Section 1: Information Technology (IT) Governance
- Section 2: Project and Service Administration
- Section 3: IT Management
- Section 4: Financial and Human Resource Management
- Section 5: Information Security
- Section 6: Risk Management
- Section 7: Facilities
- **Section 8.0: Bring Your Own Device (BYOD) Standard**
- Updates and Revisions

8.2 Applicability

Print friendly Email or share Version date October 17, 2013

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 this confidential 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 of USG data and connecting to a network.

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.

Information Technology Handbook

Search the handbook

Go

- Overview
- Introduction
- Section 1: Information Technology (IT) Governance
- Section 2: Project and Service Administration
- Section 3: IT Management
- Section 4: Financial and Human Resource Management
- Section 5: Information Security
- Section 6: Risk Management
- Section 7: Facilities
- **Section 8.0: Bring Your Own Device (BYOD) Standard**
- Updates and Revisions

8.3 Standards

Print friendly Email or share Version date October 17, 2013

8.3.1 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.

return to top

8.3.2 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.

return to top

8.3.3 USG Intellectual Property

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.

return to top

8.3.4 Device and Application Support

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.”

return to top

Information Technology Handbook

Search the handbook

Go

- Overview
- Introduction
- Section 1: Information Technology (IT) Governance
- Section 2: Project and Service Administration
- Section 3: IT Management
- Section 4: Financial and Human Resource Management
- Section 5: Information Security
- Section 6: Risk Management
- Section 7: Facilities
- **Section 8.0: Bring Your Own Device (BYOD) Standard**
- Updates and Revisions

8.4 Standard Non-Compliance

Print friendly Email or share Version date October 17, 2013

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.

Information Technology Handbook

Search the handbook

Go

- Overview
- Introduction
- Section 1: Information Technology (IT) Governance
- Section 2: Project and Service Administration
- Section 3: IT Management
- Section 4: Financial and Human Resource Management
- Section 5: Information Security
- Section 6: Risk Management
- Section 7: Facilities
- **Section 8.0: Bring Your Own Device (BYOD) Standard**
- Updates and Revisions

8.5 Appendix A: Employee Declaration

Print friendly Email or share Version date October 17, 2013

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