Clayton State University
Information Systems
BYOD Policy

July 2017

BYOD Bring Your Own Device Policy

Personally-Owned Device Usage at Clayton State University

This policy applies to any hardware and related software that is not owned or supplied by Clayton State University, but could be used to access Clayton State University resources. This applies to all Clayton State University agents who have personally acquired a device but also wish to use this device in the business environment.

All users employing a personally-owned device connected to a CSU network, and/or capable of backing up, storing, or otherwise accessing CSU data of any type, must adhere to CSU defined policies, standards, and processes.

The following definitions are used throughout this section.

1. Bring Your Own Device (BYOD): Refers to employees taking their own personal device to work, whether laptop, smartphone, or tablet, in order to interface with the internal/participant organization's network resources. This also refers to mobile storage devices such as USB drives, external hard drives, etc.

2. 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), Health Insurance Portability and Accountability Act (HIPPA), PCI standards, as well as, data not releasable under the Georgia Open Records Act, the Georgia Open Meetings Act, or some other statute.

Clayton State University
Information Systems
BYOD Policy
July 2017

3. Public Data: Data elements that have no access restrictions and are available to the general public. This data can also be designated as unrestricted data.

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

5. 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) PCI standards, as well as, data not releasable under the Georgia Open Records Act, the Georgia Open Meetings Act, or some other statute.

6. Use: Use includes accessing, inputting, processing, storing, backing up, or relocating any Clayton State University or client specific data, as well as, connecting to a network.

7. Devices: Devices include smartphones, tablets, laptops, desktops and mobile storage devices such as USB drives, external hard drives, etc.

8. Agents: Agents include employees, including full- and part-time staff, students, consultants, and other agents.

Clayton State University
Information Systems
BYOD Policy

July 2017

9. Related policies include:

· Clayton State University's Computer & Network Appropriate Usage Policy

· Section 8.0: Bring Your Own Device (BYOD) Standard of the University System of Georgia Information Technology Handbook http://www.usg.edu/information_technology_handbook/section8

Guidelines for Acquisition and Use

1. Employees and other agents must appropriately secure the device to prevent data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse to Clayton State University's computing infrastructure by following security guidelines.

a. Employ some sort of device access protection such as, but not limited to, strong passcode, facial recognition, card swipe, fingerprint, etc.

b. Set an idle timeout that will automatically lock the device if misplaced

c. Keep the device's software (operating, anti-virus, security, encryption, etc.) up-to-date

d. Enroll your device in "Find my phone" or similar services and/or label your device with some identifying information (work or home phone number, name, and or Clayton State address) to make the device easy to return if lost or stolen, this may be done via your locked screen

Clayton State University
Information Systems
BYOD Policy
July 2017

e. Report immediately to your manager 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. (Managers will immediately report such incidents to the Clayton State University's Vice President of Information Technology)

2. Sensitive and private data must not be stored on these devices or on external cloud-based personal accounts, such as Dropbox or Box.net.

3. At the time that use of the personally owned device for Clayton State business is no longer required the employee will provide documentation to their manager acknowledging and confirming that the device does not contain any Clayton State University sensitive data.

4. Employees and other agents must:

a. Complete the Information Security Training

b. Log into D2l. Click on Personally Owned Device then complete and submit the Employee Declaration. A digital record of the declaration will be maintained. As part of the completion of the form, your department code has to be entered. Since the department code definitions are updated over time if you are unsure of which department code you should, please consult the budget manager for your department.

Clayton State University
Information Systems
BYOD Policy

July 2017

Additional Considerations

1. Employees using prior approved personally owned devices may not be reimbursed by the University for purchase or for monthly service expenses. (See the Travel Policy for Long Distance and International calls reimbursement guidelines).

2. Loss, theft, or damage to personally owned devices will not be reimbursed by the University. This includes, but is not limited to, when the device is being used for University business, on University time, or during business travel.

3. Personally Owned devices used to access, store, back up, or relocate any Clayton State University or client specific data may be subject to the search and review as a result of litigation that involves the University and in accordance with the State of Georgia Open Records Act.

4. Clayton State University reserves the right to implement technology to enable the removal of university owned data and to monitor access in order to identify unusual usage patterns or other suspicious activity. This monitoring may be necessary in order to identify accounts/computers that may have been compromised by external parties.

Failure to comply with the Clayton State University's Personally Owned Device Usage policy may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.