Bring Your Own Device (BYOD) Policy

Effective Date: 07/01/2013
Last Revised: 07/01/2015
Last Reviewed: 04/07/2017

Audience

All Staff who use personal devices to access or store MBI Institutional Data

Purpose

Personal devices, including smartphones, tablet computers, and personal computers are important tools for employees as they seek to fulfill their job responsibilities at Moody Bible Institute. Due to their mobility and lack of centralized management, personal devices can produce vulnerabilities to data security. As MBI has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation, this document outlines a set of practices and requirements for the safe use of mobile devices.

Information Technology Services will administer this Bring Your Own Device policy. Issues of non-compliance with this policy will be assessed by MBI and referred to the VP of Information Technology Services for further action.

Policy

- Take appropriate measures to physically secure your device or USB storage drives (keep it with you, or locked up).
- Devices must be configured with a secure password that complies with MBI's password policy.
- Properly erase all MBI data from your device prior to discarding.
- Do not use browser "Remember My Password" feature for institutional systems (Oracle Financials, Blackboard, Campus Solutions, etc.).
- Devices must be set to auto-lock after a period of time.
- Users must report all lost or stolen devices that have MBI data on them to MBI immediately, allowing MBI to help them perform a remote wipe of the device quickly to minimize data compromise.
- If a user suspects that unauthorized access to company data has taken place via a mobile device he/she must report the incident in alignment with MBI's incident handling process.
- Users must not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

- Do not "jailbreak" or "root" your device.

Best Practices

- Store only the essential MBI Institutional data that you need, as long as it is needed, on any device.
- Devices should be kept up to date with manufacturer or network provided patches and antivirus software. At a minimum, patches should be checked for weekly and applied at least once a month.
- Label your device with a name and phone number to make the device easy to return if lost.
- Enroll your device in "Find My iPhone" or similar service to help locate the device if misplaced.
- If capable, configure the device to use hardware encryption.

Definitions

Personal Devices: Any personally owned device, including, but not limited to smartphones, tablet computers, personal computers, PDA's, Pocket PC's, mass storage devices such as thumb/jump drives, USB hard drives, IPODS and data storage tools such as Secure Digital and Compact flash transferable memory cards, used to access MBI Institutional Data.
Institutional Data: Moody information stored electronically that is not generally available to the public. This includes and is not limited to: donor names, addresses, and giving; student academic information; Social Security and credit card numbers, personal addresses, grades, medical information, other personal and financial data, and communication between Moody employees. This data should be accessed and stored only as needed to fulfill job functions. Users must delete the Institutional data from their personal device after it is no longer needed
Password protected: Requires that a password be entered to access the device or necessary if the device has been idle for a period of time. This prevents the unauthorized use of a lost or stolen device. These passwords should follow strong password guidelines defined on the password policy.
Jailbreak / Rooting device: Jailbreaking or rooting is a device hack that provides users with unrestricted access to the entire file system of their mobile devices and allows the user to modify the root operating system running on mobile devices to allow the user greater control over his or her device.
Media Files: Audio files/iTunes libraries, videos, pictures, and mobile phone backups.

Procedures

n/a

Documents

n/a

Contacts

If you have questions or concerns about the execution of this policy, you may contact the Information Technology Services Support Center at 312.329.4067 or ITS@moody.edu for assistance.

If you have questions about the policy, you may email ITSpolicy@moody.edu for assistance.

Related

- n/a