MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
BRING YOUR OWN DEVICE – 1:08:00:05
Approval
Corresponding Policies: TBR Guidelines G-051; G-052
Leadership Council Approved: April 13, 2018
Effective Date/Approved: April 13, 2018
Revised: N/A
Responsible Party: Chief Information Officer

I. PURPOSE

A. The purpose of this policy is to protect and ensure the integrity of the Motlow State Community College network and institutional data on personal devices not owned by Motlow.

B. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an unsecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of student or employee information, damage to critical applications, and damage to the institution's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Motlow's direct control to backup, store, and otherwise access Motlow-owned data of any type must adhere to college-defined processes for doing so.

II. APPLICABILITY

A. This mobile device policy applies to, but not limited to, all devices and accompanying media that fit the following device classifications:
1. Laptop/notebook/tablet computers
2. Ultra-mobile PCs (UMPC)
3. Mobile/cellular phones
4. Smartphones
5. Media players such as iPods
6. Digital or video cameras
7. Personal Digital Assistants (PDAs)
8. USB hard drives
9. CD-R or DVD-R media
10. Peripheral devices connected to a mobile device
11. Home or personal computers used to access institutional resources
12. Any mobile or peripheral device capable of storing Motlow-owned data and connecting to an unmanaged non-Motlow network

B. The policy applies to any personally-owned hardware and related software that is used to access institutional resources.

C. This policy applies to all Motlow State Community College employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile

devices to access, store, back up, relocate or access any department or student-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Motlow has built with its students, employees and community. Consequently, employment at Motlow does not automatically guarantee the initial and ongoing ability to use these devices to gain access to institutional networks and information. Information Technology (IT) addresses a range of threats to – or related to the use of – institutional data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive institutional data is deliberately stolen and sold.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the college to the risk of non-compliance with various identity theft and privacy laws.

III. ACCEPTABLE USE POLICY

It is the responsibility of any employee of Motlow who uses a mobile device to access institutional resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct college business be in accordance with the Motlow State Community College acceptable use guidelines outlined in Motlow's Policy 1:08:00:00 (Information Technology Resources). Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

IV. ACCESS CONTROL

Motlow reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to institutional and institutional-connected systems. Motlow will engage appropriate access control actions if it feels a mobile device is being used in a way that puts the college's network, hardware, software, data, employees, or students at risk.

i.

V. METHODS OF SECURITY AND PROTECTION

A. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. Suggested methods of security and protection are:
   1. Encrypt or password protect all data owned by the college
   2. Use network shared drives, which are secured an only allow authenticated user access
   3. Use virtual private networks (VPN), which provide secure and encrypted connections to the college's network and data
   4. Use tracking and recovery software to enable the identification and retrieval of the device in the event of theft or loss
   5. Use device security locks, which may include password, pin or biometric security
   6. Use anti-virus and anti-malware protection
   7. Disable unused services, such as wireless, infrared or Bluetooth when not in use
   8. Avoid unencrypted storage of usernames and passwords
   9. Avoid usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties

10. Any non-college computers used to synchronize with these devices will also conform to the methods of security and protection listed above.

VI. ACCESS AND STORAGE OF SENSITIVE COLLEGE INFORMATION

A. All mobile devices used to access or store sensitive college information must meet the following requirements:
   1. Unencrypted sensitive information should not be stored on mobile devices but may be accessed via the college network by utilizing a secure VPN access
   2. Sensitive college information should never be stored on personal mobile devices and sensitive information accessed via email should be removed from mobile devices as quickly as possible
   3. The use of encrypted or unencrypted USB drives (i.e. “flash drives”, “thumb drives”) and portable hard drives for storing sensitive college information is strongly discouraged because of their vulnerability to viruses and ransomware. Recommended alternative storage solutions include:
      a. Microsoft OneDrive
      b. Google Drive
      c. Dropbox
      d. Apple iCloud Drive
   4. Mobile devices used to access or store sensitive college information must not be left unattended and should be physically locked away or secured
   5. Mobile devices containing sensitive college information should never be shared with any unauthorized user
   6. The owner of any mobile device containing sensitive college information should always take reasonable care when using the device in public places or other unprotected areas in order to avoid unauthorized access or disclosure of information stored on the device

VII. TERMINATION OF COLLEGE RELATIONSHIP

Employees, contractors, and temporary staff must erase all college related data permanently from personally owned mobile devices upon termination of the assigned user’s relationship with the college. In addition, any software applications purchased by the college and installed on a personal mobile device must be removed by the user.

VIII. REPORT OF LOSS, THEFT OR SUSPECTED MISUSE

In the event of any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks or in the event of a lost or stolen mobile device, it is incumbent on the employee to report this to Motlow’s IT department immediately. IT will attempt to remotely wipe all data and lock the device to prevent access by anyone other than IT.

IX. HELP & SUPPORT

A. Motlow’s IT Department will not provide support for unsanctioned hardware and software issues on personally-owned devices. Sanctioned software on a personally-owned device will be supported on a limited case-by-case basis depending on availability and discretion of technical staff.

B. Employees, contractors, and temporary staff will make no modifications of any kind to Motlow-owned and installed hardware or software without the express approval of Motlow’s IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

C. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.