MONTGOMERY COUNTY
TENNESSEE

Personal Mobile Device Acceptable Use Policy
08/01/12

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business uses for connecting a personally-owned mobile device to Montgomery County's corporate network. This mobile device policy applies, but is not limited, to all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- E-readers
- Portable media devices
- PDAs
- Portable gaming devices
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers
- Any mobile device capable of storing corporate data and connecting to a network

The policy applies to any hardware and related software that is not corporately owned or supplied, but could be used to access corporate resources. That is, devices which employees have purchased for personal use but also wish to use in the business environment.

The overriding goal of this policy is to protect the integrity of the confidential client and business data that resides within Montgomery County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a mobile device connected to Montgomery County's corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes for doing so.

Applicability

This policy applies to all Montgomery County employees, including full and part-time staff, contractors, interns, and other agents who use a personally-owned mobile device to access, store, back up, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Montgomery County has built with its clients, supply chain partners, and other constituents. Consequently, employment at Montgomery County does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to, or related to the use of, enterprise data:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party.
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 enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of Information Systems. **Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.**

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the enterprise network.

Responsibilities

The Director of Information Systems of Montgomery County has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

The Mayor of Montgomery County has delegated the execution and maintenance of information technology and information systems to Director of Information Systems.

Other Information Systems staff, under the direction of the Director of Information Systems, is responsible for following the procedures and policies within Information Systems.

All Montgomery County employees are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by Montgomery County's Information Systems department and will use authentication and strong encryption measures. Although Information Systems will directly manage personal devices, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the County's infrastructure.

Policy and Appropriate Use

It is the responsibility of any employee of Montgomery County who uses a mobile device to access corporate 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 Montgomery County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Access Control

- Information Systems reserves the right to refuse, by physical and non-physical means, the ability to connect personal mobile devices to corporate and corporate-connected infrastructure. Information Systems will engage in such action if such equipment is being used in a way that puts the company's systems, data, and users at risk.

- Prior to initial use on the corporate network or related infrastructure, **all mobile devices must be approved by Information Systems.** Montgomery County will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored at http://www.mcgtn.org/information-systems . Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the help desk 931-648-5778. Although Information Systems currently allows only listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in future.

- End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data **must employ**, for their devices and related infrastructure, security measures deemed necessary by the Information Systems department. Enterprise data is not to be accessed on any hardware that fails to meet Montgomery County's established enterprise Information Systems security standards.

- All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected using technology centrally managed by Montgomery County's Information Systems department. Devices that have not been previously approved by Information Systems are not in compliance with Information Systems' security policies, or represent any threat to the corporate network or data will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones, tablets, and UMPCs will access the corporate network and data using mobile VPN software installed on the device by Information Systems.

Security

- Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. **All mobile devices must be protected by a strong password**; a PIN is not sufficient. All data stored on the device must be encrypted using **strong encryption**. See Montgomery County's password and encryption policy at http://www.mcgtn.org/information-systems for additional background. Employees agree to never disclose their passwords to anyone, even to family members, if business work is conducted from home.

- All users of mobile devices **must employ reasonable physical security measures**. End users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.

- Any non-county computers used to synchronize with these devices will have installed **up-to-date anti-virus and anti-malware software deemed necessary** by Montgomery County's Information Systems department. See http://www.mcgtn.org/information-systems for anti-virus requirements and recommendations.

- Passwords and other confidential data as defined by Montgomery County's Information Systems department are **not to be stored unencrypted** on mobile devices.

- Any mobile device that is being used to store Montgomery County data must **adhere to the authentication requirements** of Montgomery County's Information Systems department. In addition, all hardware security configurations must be pre-approved by Montgomery County's Information Systems department before any enterprise data-carrying device can be connected to the corporate network.

- Information Systems will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. **Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt** and will be dealt with in accordance with Montgomery County's overarching security policy.

- Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to **permanently erase company-specific data from such devices once its use is no longer required**. See http://www.mcgtn.org/information-systems for detailed data wipe procedures for mobile devices.

- In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to Information Systems immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than Information Systems. This action will restore the device to its factory default settings. If the device is recovered, it can be submitted to Information Systems for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to county business or personal. This data is not recoverable on the device itself, but can usually be restored from a backup on another device (e.g. a personal computer) if the mobile device remains in or returns to the users possession or a new device is able to store the backup.

    - It is recommended that users back up their personal data frequently to minimize loss if a remote wipe is necessary. By signing this document the user understands that their personal data may be erased in the rare event of a security breach, must be agreed with before connecting the device to corporate resources. When a remote wipe is initiated by the Information Systems department, the user's mobile device will be wiped of all data and restored to its factory default settings. The wipe is not limited to County data. Data that the employee has added to the device for personal use will also be deleted. This data is not recoverable on the device itself, but can usually be restored from a backup on another device (e.g. a personal computer) if the mobile device remains in or returns to the users possession or a new device is able to store the backup. It is recommended that users back up their personal data frequently to minimize loss if a remote wipe is necessary.

- Examples of situations requiring remote wipe include, but are not limited to:
    - Theft of the device.
    - Loss of the device.
    - Termination of employment in which the user has not already cleared corporate data by another method.
    - Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
    - Non-Business usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

Help & Support

- Information Systems 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.
- Employees, contractors, and temporary staff will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system) without the express approval of Montgomery County's Information Systems department.

Organizational Protocol

- Information Systems can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. **The end user agrees to and accepts that his or her access and/or connection to Montgomery County's networks may be monitored to record dates, times, duration of access, etc., 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.
- The end user agrees t**o immediately report** to his/her manager and Montgomery County's Information Systems department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.
- Montgomery County may reimburse employees for phone/data plans if they choose to purchase their own mobile devices.
    - Users will be given a stipend to cover basic mobile network usage costs and/or phone plan **up to $50 per month**. Reimbursement eligibility will be determined by each Department Head/Elected Official's discretion depending on job and mobility requirements. Reimbursement details are available at Human Resources.

- Every mobile device user will be entitled to, and expected to attend, a training session about this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

- Any questions relating to this policy should be directed to Kurt Bryant in Information Systems, at kmbryant@mcgtn.net. A copy of this policy can be found at www.mcgtn.org/human-resources/policies.

Policy Non-Compliance

Failure to comply with the *Personal Mobile Device Acceptable Use Policy* may, at the full discretion of the county, result in the **suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment**.
The Immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action.

Confidentiality

Any county employee utilizing personal mobility device(s) as defined in this policy to access the Montgomery County network maybe subject to the Open Records law of Tennessee pursuant to T.C.A. Title 10 Chapter 7 or other applicable provisions thereof.

Employee Declaration

I, [employee name], have read and understand the above *Personal Mobile Device Acceptable Use Policy*, and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
Department Head/Elected Official Signature	Date
_____	_____
Information Systems Director Signature	Date

.