



REQUEST FOR BOARD ACTION

ITEM NO. 13.

DATE OF MEETING: December 3, 2012

REQUESTED BY: Erik Harvey, Director, ITS Department

SHORT TITLE: Resolution Authorizing Adoption of Mobile Acceptable Use Policy

BACKGROUND: The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a County provided and personally-owned device to Pender County's network for business purposes. This device policy applies, but is not limited to, all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

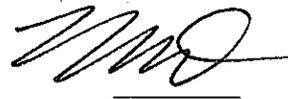
- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing organizational data and connecting to a network

The policy applies to any hardware and related software that is Pender County owned and personally-owned or supplied, but could be used to access county resources. That is, devices which employees have acquired 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 Pender County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a 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 Pender County's public image. Therefore, all users employing a personally-owned device connected to Pender County's network, and/or capable of backing up, storing, or otherwise accessing county data of any type, must adhere to Pender County defined processes for doing so.

SPECIFIC ACTION REQUESTED: To consider a resolution adopting the Mobile Acceptable Use Policy.

COUNTY MANAGER'S RECOMMENDATION

Respectfully recommend approval.


Initial

RESOLUTION

NOW, THEREFORE, BE IT RESOLVED by the Pender County Board of Commissioners that

the Mobile Acceptable Use Policy be authorized. The Chairman/County Manager is authorized to execute any and all documents necessary to implement this resolution.

AMENDMENTS:

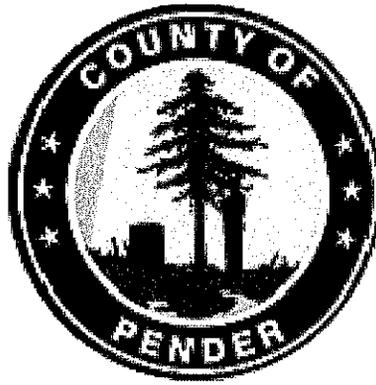
MOVED _____ SECONDED _____

APPROVED _____ DENIED _____ UNANIMOUS _____

YEA VOTES: Brown ___ McCoy ___ Tate ___ Ward ___ Williams ___

Chairman 12/03/12
Date

ATTEST 12/03/12
Date



Pender County

Mobile Acceptable Use Policy

Effective Date: December 3, 2012

Pender County Information Technology Services
805 S. Walker Street
Burgaw, NC 28425
910-259-1260

Table of Contents

1. Purpose	3
2. Applicability	4
3. Responsibilities	5
4. Affected Technology	5
5. Stipend Guidelines	5
6. Policy and Appropriate Use	6
7. Access Control	6
8. Security	7
9. Help & Support	8
10. Organizational Protocol	8
11. Employee Declaration	9
12. Policy Non-Compliance	10

Pender County

Mobile Acceptable Use Policy

I. Purpose:

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a County provided and personally-owned device to Pender County's network for business purposes. This device policy applies, but is not limited to, all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing organizational data and connecting to a network

The policy applies to any hardware and related software that is Pender County owned and personally-owned or supplied, but could be used to access county resources. That is, devices which employees have acquired 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 Pender County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a 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 Pender County's public image. Therefore, all users employing a personally-owned device connected to Pender County's network, and/or capable of backing up, storing, or otherwise accessing county data of any type, must adhere to Pender County defined processes for doing so.

II. Applicability:

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

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

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive county 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 devices.
Compliance	Loss or theft of financial and/or personal and confidential data could expose Pender County 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 device connectivity will be managed at the sole discretion of IT. **Non-sanctioned use of personal 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 county network.

III. Responsibilities:

The County ITS Department has the overall responsibility for the confidentiality, integrity, and availability of county data.

The Board of County Commissioners and County Manager of Pender County has delegated the execution and maintenance of information technology and information systems to the ITS Director.

Other departmental IT staff under the direction of the ITS Director are responsible for following the procedures and policies within information technology and information systems.

All Pender County employees are responsible for acting in accordance with county policies and procedures.

IV. Affected Technology:

Connectivity of all employee-owned devices will be centrally managed by Pender County's ITS department and will use multi-factor authentication and strong encryption measures or alternative compensating controls to isolate and protect any county data accessed from or stored on the device where appropriate. Although the IT department will not directly manage personal devices, end users are expected to adhere to the same

security protocols when connected to non-county equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the county's data and network infrastructure.

V. Stipend Guidelines:

Pender County will provide a stipend to an eligible employee that can be used for both business and personal purposes. All devices must be approved by the ITS Department before purchase. The stipend will be set at 50% of the average cost that would have been incurred for voice and data charges with a Pender County provided phone not to exceed the employee's actual base monthly charge.

1. The cell phone stipend is set at \$20.00/month versus the current average cost of \$40/month.
2. The smartphone stipend is set at \$35.00/month versus the current average cost of \$70.00/month.
3. If the user has a County issued cell phone or smartphone it must be turned in prior to the new phone being connected to County resources by the IT Department.
4. Stipend amounts are nontaxable; user may elect to not receive stipend.
5. The County may require users to publish their personal phone number for on-call support or other job requirements.

This stipend is intended to cover:

1. The cost of the device
2. Operating system
3. Required business productivity applications
4. Anti-virus software
5. Service contract

The employee is responsible for all initial and subsequent acquisition costs associated with a personally-owned device i.e. cell phone or smartphone. The employee may exceed the stipend amount at their own expense.

In the event of termination, retirement, or resignation, the employee must reimburse a prorated amount of the stipend. The prorated amount is based on the number of monthly or quarterly cost remaining on the employee's personally-owned device service contract. The amount due will be gathered from the final pay where possible or, if not, charged to the employee to be collected within 30 days of the last day worked.

Pender County reserves the right to modify the stipend at any time it deems necessary.

VI. Policy and Appropriate Use:

It is the responsibility of any employee of Pender County who uses a personal device to access business 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 Pender 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:

VII. Access Control:

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect personal devices to county network and non-county networks. IT will engage in such action if such equipment is being used in a way that puts Pender County IT systems, data, users, and clients at risk.
2. Prior to initial use on the Pender County network (s) or related infrastructure, **all devices must be approved by IT**. Pender County will maintain a list of approved technologies with associated control requirements. Devices that are not on the approved list may not be connected to the county network. If your preferred device does not appear on this list, contact the IT help desk at 910-259-1260. Although IT currently allows only listed devices to be connected to county network, it reserves the right to update the list in future.
3. County data is not to be stored on or accessed from any hardware that fails to meet Pender County's established enterprise IT security standards.
4. All personal devices attempting to connect to the Pender County network through the Internet will be inspected using technology centrally managed by Pender County's ITS Department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the county network or data will not be allowed to connect. Devices may only access the county network and data through the Internet using an IPSec or SSL 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 county network and data using mobile VPN software installed on the device by IT.

VIII. Security:

Employees using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. **All devices that are able to store data 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 Pender County's Password policy for additional information. Employees agree never to disclose their passwords to anyone, including family members, or store passwords on personally-owned devices if county work is conducted from home.

1. All users of personally-owned 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.

2. Any non-business computers used to synchronize with these devices will have installed **up-to-date anti-virus and anti-malware software deemed necessary** by Pender County's IT department.
3. Passwords and other confidential data as defined by Pender County's IT department are **not to be stored unencrypted** on mobile devices.
4. Any device that is being used to store Pender County data must **adhere to the authentication requirements** of Pender County's IT department. In addition, all hardware security configurations must be pre-approved by Pender County's IT department before any county data-carrying device can be connected to the county network.
5. IT 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 Pender County's Employee Personnel Policies.
6. 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 county network.
7. Employees, contractors, and temporary staff will follow all county-sanctioned data removal procedures to **permanently erase county-specific data from such devices once its use is no longer required**.
8. In the event of a lost or stolen device, it is incumbent on the user to report the incident to IT immediately. The device **will be remotely wiped** of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. **Appropriate steps will be taken to ensure that Pender County data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device**, whether it is related to county business or personal.

IX. Help & Support:

1. Employees who opt in to the BYOD program are not eligible for support for device-specific hardware or software from Pender County's IT department. If the employee-owned device requires maintenance, the employee is responsible for taking the device to an employee-provided third party as covered by the stipend or business-approved third party support provider.
2. The IT department will triage support calls to determine if the issue is software or hardware related. If the issue is hardware related, the employee will be forwarded

to the third-party support provider for maintenance. If the issue is software related or related to virtual or web-based applications, the IT department will perform maintenance.

3. 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 or "jail-breaking") without the express approval of the IT department.

X. Organizational Protocol:

1. IT 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 County's 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 Pender 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. The employee consents that there is no right to privacy related to use of organizational networks, resources, or data.** This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties.
2. The end user agrees to **immediately report** to his/her manager and the IT department **any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.**
3. While a personally-owned device user will not be granted access to county resources 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. By signing this policy, employees acknowledge that they fully understand the risks and responsibilities of the BYOD program.
4. Any questions relating to this policy should be directed to the IT department, at 910-259-1260.

XI. Policy Non-Compliance:

Failure to comply with the *Mobile 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, possible termination of employment, as well as possible criminal charges.**

The County Manager, ITS Director, and immediate Department Head and/or Supervisor will be advised of breaches of this policy and will be responsible for appropriate remedial action.

XII. Employee Declaration

I, _____ have read and understand the above *Mobile Acceptable Use Policy*, and consent to adhere to the rules outlined therein.

Employee Signature Date

Department Head Signature Date

ITS Director Signature Date