*INCORPORATED COUNTY OF LOS ALAMOS*
*ADMINISTRATIVE PROCEDURE GUIDELINE*

Index No. 1240 Effective Date: October 7, 2012

# LOS ALAMOS COUNTY
# PERSONAL MOBILE DEVICE ACCEPTABLE USE POLICY

## I. 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 Los Alamos County's (LAC) corporate network and choose to do so. Foremost, the purpose is to protect the integrity of the confidential data that resides within LAC's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored in an unsecured method on a mobile device or carried over an unsecure network where it could potentially be accessed by unauthorized entities.

## II. Policy

It is the policy of LAC that any employee who uses a personal mobile device to access LAC resources ensures security protocols are used in the management of data. Employees that utilize personal mobile devices while conducting LAC business shall do so in a professional manner and shall provide all County records to the County in accordance with County policy 0310 – Records and Information Management Governance Policy.

The following shall be observed:

A. Prior to consideration of mobile device usage on LAC network or applications, requests for mobile access must be approved and submitted to Information Management (IM) by employee's supervisor. Supervisor consideration shall be consistent with Personnel Rules and Regulations (which may be amended from time to time) as well as other LAC policies.

B. Some devices, depending upon type and operating system, may or may not be able to integrate with the LAC network. IM will maintain a list of accepted mobile platforms known to integrate with LAC's network. This list will be updated periodically.

C. End users who wish to connect mobile devices to non-LAC network infrastructure to gain access to enterprise data must employ LAC approved VPN for their devices. Enterprise data is not to be accessed on any hardware that fails to meet LAC's established enterprise IM policies.

D. All mobile device connections to the LAC network through the Internet shall come through automated technology which will inspect the personal device including data and applications on that device. The automated technology will be centrally managed by IM. The automated technology is not configured to keep a log of applications and data on the device.

E. In order to secure data management, the following shall be adhered to with regard to security:

1. Employees using mobile devices and related software for network and data access shall use secure data management procedures and reasonable physical security measures as outlined in 1210-IT Security and Usage Policy (which may be amended from time to time).

2. Any mobile device that is being used to store LAC data must adhere to the authentication requirements (e.g., login credentials, smart cards, fobs, certificates, etc.) of LAC and other applicable agreements, (i.e., end user license agreements, joint powers agreements, etc.) regulations and laws. In addition, all hardware security configurations must be pre-approved by taking to IM for inspection before any enterprise data-carrying device can be connected to the LAC network.

3. IM will manage security policies, network, application and data access centrally using automated technology. Any attempt to bypass security implementations will be deemed an illegal or improper intrusion attempt and will be dealt with in accordance with 1210-IT Security and Usage Policy (which may be amended from time to time).

4. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase County data from such devices once its use is no longer required. Before an employee discontinues use of a device for work purposes or disposes of the device, it is the employee's responsibility to either remove County data from the device and notify IM that they have done so or contact IM for help in removing the data which may include a request that the device be wiped remotely. In the event that the employee does not notify IM that they have permanently erased County data from their device, the device will be wiped remotely upon notification to IM that the staff member no longer works for the County.

5. In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to IM prior to contacting the mobile device vendor so appropriate data wipe activities can occur. This should be done immediately when the device is noticed missing. The device will be remotely wiped of all data and locked to prevent access by anyone other than IM. If the device is recovered, it can be submitted to IM for re-provisioning. The LAC Remote

Wipe Waiver, which ensures that the user understands that their personal data shall be erased in the rare event of a security breach, shall be agreed to in writing before connecting the device to LAC resources.

## III. Help and Support

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

B. 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 written approval of IM.

## IV. Organizational Protocol

A. IM establishes audit trails, which will be accessed, produced and used as may be required by law. Such trails will be able to track the attachment of an external device to the LAC network, and the resulting reports may be used for investigation of possible breaches and/or misuse or for any other reason deemed appropriate by the County. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties. As part of the written waiver, the end user agrees that his or her access and/or connection to LAC's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.

B. The end user agrees to immediately report to his/her manager and IM any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of County resources, databases, networks, etc.

## V. Responsibility

A. Connectivity of all mobile devices will be centrally managed by LAC's IM Division and will use authentication and strong encryption measures. Although IM will not directly manage personal devices which connect to the LAC network, end users are expected to secure these devices when connected to non-LAC networks/resources (see Section 2.5.5 and 2.7 for additional information). Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed by IM. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is prohibited.

B. This policy applies to all LAC employees, including full and part-time staff, contractors, and other agents who use a personally-owned mobile device to access, store or back up any LAC data. LAC does not automatically guarantee the initial or ongoing ability to use these devices to gain access to LAC networks and information.

C. This mobile device policy applies to all LAC-supported devices.

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

VI. Violations

A. Failure to comply with this policy may result in immediate suspension of that user's account. A breach could result in loss of information, damage to critical applications, loss of revenue, and damage to the LAC public image. Therefore, all users employing a mobile device connected to LAC's network, and/or capable of backing up, storing, or otherwise accessing LAC data of any type, must adhere to the LAC-defined processes for doing so.

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 LAC 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 LAC to the risk of non-compliance with various identity theft and privacy laws. |

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

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.

Failure to comply with the *Personal Mobile Device Acceptable Use Policy* may, at the full discretion of LAC, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

## VII. Definitions

| | |
|---|---|
| **Enterprise Data** | Any information, whether a record or elements that can create a record, used in conjunction with LAC business, shared by many users throughout the organization. |
| **Mobile Device** | Any portable electronic device used to store information and communicate within/outside of LAC resources; SmartPhone, tablet PC, laptop |
| **SSL** | Secure Socket Layer are cryptographic protocols that provide communication security over the Internet. |
| **VPN** | Virtual Private Network is used to privately interconnect remote users through public communication infrastructure in a secure method. |

10/4/13

HARRY BURGESS
COUNTY ADMINISTRATOR

DATE