| | |
|---|---|
| **Title** | **Mobile Device Security Policy** |
| **Type** | Policy |
| **Category** | Security |
| **Status** | Approved |
| **Approved** | 02/15/2013 |
| **Revised** | 06/16/2015 |
| **Scope** | The purpose of this policy is to comply with federal regulations governing privacy and security of information, and to protect Confidential Data in the event of laptop computer or mobile electronic data device theft. |
| **Policy** | This policy describes the minimum security for the City of Albuquerque mobile devices. Mobile devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the City of Albuquerque's computing and information infrastructure. This policy only covers City of Albuquerque owned mobile devices. Personal owned devices are covered under the Bring Your Own Device (BYOD) policy.<br><br>**1. Password Protected**<br>Whenever possible, all mobile devices must be password protected. Choose and implement a strong password. Password shall follow Security Standard "Password".<br>**2. Responsibility**<br>The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible.<br>**3. Protection of Confidential Data**<br>Every user of laptop computers or other electronic data mobile devices must use reasonable care, as outlined in the City's Information Technology Protection Policy, to protect the Confidentiality, Integrity and Availability of City Data. Protection of Confidential Data against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include user care and a combination of technical protections such as authentication, encryption, and remote access capability that work together to |

secure mobile devices against unauthorized access. Prior to use or display of Confidential Data via laptop computer or other electronic data mobile device, the following security measures must be in place.

- A laptop or other electronic data mobile device must authenticate the user before access to services on or by the device shall be permitted. Mobile devices must be configured to timeout after 15 minutes of inactivity and require re-authentication before access to services on or by the device will be permitted.
- The authentication mechanism(s) must not be disabled. The City approved encryption option must be enabled on laptop computers that transmit or store City confidential information. Laptops shall be protected with antivirus software and updated daily if supported by the device. The use of unprotected mobile devices to access or store Confidential Data is prohibited regardless of whether the equipment is owned or managed by the City. The Department of Technology and Innovation (DTI) can be contacted to determine if appropriate protections are already in place or assist with enabling the security measures for laptops or other electronic data mobile devices. Encryption of hard drive is required to store sensitive or City owned data on mobile device.

**4. Reporting Loss/Theft of Equipment or Data**

City employees who possess City owned laptop computers and other portable electronic devices are expected to secure them whenever they are left unattended. In the event a City-owned or controlled laptop computer or other device is lost or stolen, the theft or loss must be reported immediately to the Department of ownership and the Albuquerque Police Department. In the event City Confidential Data is contained on any personally-owned computer or device that is lost or stolen, DTI Service Desk must be contacted immediately.

The City reserves the right to remotely wipe the mobile device in the event of device being stolen, termination of the employee or other violation of City IT policy.

**Rationale**

Also refer to:

- Security Policy “User ID Security”
- Security Standard “Password”