Title	**Bring Your Own Device (BYOD)**
Type	Policy
Category	Security
Status	Approved
Approved	05/08/2013
Reviewed	06/15/2015
Scope	This policy applies to all personal owned mobile devices which are used for City of Albuquerque business to include, PDA's, tablets, laptops and Smartphone's capable of executing computer code and storing confidential or personal identifiable information (PII) and becoming compromised.

Policy

Definitions – Terms Specific to the Policy

Personal mobile device – A non-City owned multi-functional computing and communications device used to conduct City business that is capable of hosting a broad range of applications both for business and consumer use. Personal mobile devices include, but are not limited to personal digital assistants (PDA's), smartphones, tablets, notepads, and laptop computers.

City business – All work performed on an electronic device that has a direct relation to the City's operations and activities. City business includes any work performed where non-transient public records may be created, transmitted, or stored using a personal mobile device.

Transient records – Transitory materials consist of those records that are created primarily for the informal communications of information, as opposed to communications designed for the perpetuation of formalization of knowledge. Transitory materials include correspondence of little or limited reference value, transmittals and informational messages. Transitory messages do not set policy, establish guidelines or procedures certify a transaction, or become a receipt. Transient records may include, but are not limited to, the following types

of communications as it relates to a project or event:

- Personal notes outlining an oral report
- Preliminary drafts
- Memos (paper or electronic) pertaining to scheduling an event
- Documents designated as updated`

Mobile Device Management - Mobile device management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises.

Acceptable use

The owner of the device is responsible for the secure use of this device and the security of data on the device.

Personally or affiliate owned computers used by City affiliates, contractors, and staff for City business must comply with all City security standards. It is the responsibility of the user to ensure the required security controls are implemented and maintained in accordance with the **City Mobile Device Security Policy**.

Illicit and pornographic materials are not permitted on personal devices being brought in and connecting to the City infrastructure. **(See Employee Internet Use policy)**

Peer-to-Peer file sharing /Bit torrent applications are prohibited on the City network. These programs are configured by default to "share out"; that is, not only can you retrieve files from other users' computers, but they can retrieve files from your computer without your knowledge. **(See Standard Peer-to-Peer (P2P) Internet-based Applications)**

Illegal/pirated software is prohibited on a device that is being used for work related activity.

All existing City policies apply to employee conduct when accessing the Internet on personal owned mobile devices used to conduct City business, especially those that deal with

intellectual property protection, privacy, misuse of City resources, sexual harassment, data security, and confidentiality. **(See Employee Internet Use Policy)**

Device selection

The City of Albuquerque current standard platforms for mobile devices are the Android, IPhone, BlackBerry and IPad. Although recommended, this list does not limit the devices which are allowed. Additional devices shall be approved by the CIO or his designee.

Protection of the Device

Security Software: Prior to gaining access to the City networked resources, it is the responsibility of the owner of the device to update anti-virus and security patches when patches are available. Many older devices do not support updates. When feasible, replace these devices with newer technology that support updates.

Encryption: Devices can have built-in encryption capabilities or use commercially available encryption tools. Encryption must be enabled for any device which processes and stores City owned Personal Identifiable Information or data which may be harmful to the City if it is lost or stolen.

Password: The device should, at minimum, have a log on password, Personal Identification Number (PIN) or Pattern screen lock for authentication. Mobile devices connecting to the City network shall adhere to the City password standard.

Wi-Fi: Not all public Wi-Fi locations can be trusted. Employees shall not send sensitive data over networks that are not secure. Transaction shall be sent over a HTTPS secure connection. Additionally, Staff is encouraged to implement VPN software so that employees can connect to corporate data and resources over encrypted channels.

Use of Personal Devices Connecting to the City Network

City personnel may use personal devices, such as Ipads, tablets, laptops or desktop computers to connect to the City's network using the City's remote access facility, such as its Virtual Private Network (VPN).

If the City requires an employee or, if the employee voluntarily uses a personal mobile device for city business, at that time, a public record has been created. (e.g., text messages, photographs, voice mail, etc).

A City of Albuquerque employee, who uses a personal mobile device, either required or voluntarily to processes and stores City data, must comply with an Inspection of Public Records (IPRA) request.

In the case of an employee's refusal to comply with an IPRA request, a lawsuit can be brought and enforced if the city requires an employee or if the employee voluntarily uses a personal mobile device for city business. A court can order the production of these public records requested from the employee's personal mobile device.

Security Requirements: City personnel who use a personal device to connect to the City's network must protect their device by adhering to the City Password standard. The device must be set such that re-entering of the password is required after 15 minutes of idle time, use active and up-to-date anti-malware software, and stay current on software patches. (See Mobile Device Security Policy)

Jail-broken Devices: Jail-broken or rooted devices are devices which have been tampered with such that all limitations have been removed. City personnel may not use jail-broken or rooted devices to connect to the City's network. At no time shall a City owned device be jail-broken or rooted.

Loss of a device or leaving the City

Upon completion of employment or contract with the City, the individual is responsible for returning all equipment, software and information provided by the City, whether in electronic form or otherwise. It is the responsibility of the owner of the device to transfer all City related business to the immediate supervisor or point of contact. It is the responsibility of the individual to remove all City data stored from the device.

If the device is lost or stolen, it is the responsibility of the owner to report this loss immediately to the DTI Service desk, and the police.

Reimbursement

Unless specifically approved by the department manager, the City will not reimburse staff for the use of personally owned devices.

Support Expectations:

Personnel who choose to use a personal mobile device to conduct City business must not expect City IT staff to support personal mobile devices.

Mobile device management

The implementation of Mobile device management (MDM) software lets IT configure, secure, monitor and wipe smartphones and tablets and other mobile devices. MDM is also one element that can enforce BYOD policy and other requirements. The City reserves the right to implement a MDM strategy in protecting City resources in securing mobile devices connecting to the City infrastructure.

Agreements

All personnel using personal mobile devices for conducting City Business are responsible for adhering to this policy. Any violation of this policy is subject to loss of privileges and disciplinary action up to and including termination.

Rationale

The goal of the City of Albuquerque “Bring Your Own Device” or BYOD is to make BYOD use feasible by seamlessly securing corporate data and applications on the device while providing a logical separation from personal activities and data. Each City employee is responsible for the security of City of Albuquerque data.