THE CITY OF LAKE FOREST **ADMINISTRATIVE DIRECTIVE 2-4a**
Office of the City Manager **May 2017**

USE OF PERSONAL MOBILE DEVICES FOR CITY BUSINESS (BYOD)

1.0 Purpose:

The purpose of this directive is to establish policies and guidelines for employees to use personal mobile devices to access the City network in the performance of their job duties.

2.0 Scope:

All City employees and contracted employees (Employees) who use a personally owned mobile device to perform their duties to the City.

3.0 Definitions:

User - Employees or contract employees connecting to the City data network with a personal mobile device.

Device – A device is any personal mobile device, internet-enabled cell phone, tablet, laptop computer or other portable electronic device when used to access any part of the City's network as described below. This may also be referred to as Bring Your Own Device (BYOD).

Network Access –Network access includes accessing the City's internal wireless access points (Wi-Fi), the Virtual Private Network (VPN) and physically connecting a device to the City network physically via a cable.

Compromised Device – A compromised device is a device that is hacked, has had its security penetrated, has been accessed by an unauthorized individual, has been infected by a virus or malware, or whose data has been wrongfully obtained by a third party.

4.0 Policy:

4.1. Authorized Users. The use of personally owned devices is not required by the City, but does present obvious advantages to both the City and its employees. Only employees authorized by their executive level department head may use personally owned devices to connect to the City network to perform their duties.

Authorization to connect to the City network in either manner may be rescinded at any time, for any reason, without prior notice.

4.2 Authorized Devices. Some makes and models of personal devices or their associated operating systems may present an unacceptable security risk to the City network. Therefore the City's Assistant Director IT Division may prohibit the use of any such devices or operating systems they feel necessary to protect the City network. No device may ever be "jail broken" (IOS) or "rooted" (Android), or have software or firmware installed that is designed to gain access to prohibited applications.

The Assistant Director IT Division shall have the discretion to determine which makes and models (if any) of devices and/or which versions of operating systems are unauthorized, maintain a list of unauthorized devices and/or operating systems, and shall have the discretion to de-authorize a previously authorized or approved device if it is deemed to be a security risk to the City.

4.3 Authorized Purposes/Scope of Access to Network. Any user using their device to access the City network to perform work in any way is subject to all administrative directives governing such use, including but not limited to directive 2-4 ("Electronic Communications System Policy") and directive 2-16 ("Cell Phone Use"). A user using their device may not access those portions of the City's network they are not normally authorized to access.

4.4 Monitoring of Devices When Connected to City Network. Whenever any user is connected to the City network the City may monitor, record and preserve any data passing through the City network. A user acknowledges that he/she has no expectation of privacy to data transmitted in this fashion including, but not limited to, files, pictures, emails, text or IM messages, internet activity history or any other such transmitted data.

4.5 Device Security and Data Backup. See Administrative Directive 2-4 for PIN/password requirements. The City will not backup data created or stored on a user's device. The City strongly encourages users to save all work related material to the City's network, rather than on their BYOD device.

4.6 Lost and Compromised Devices. Users must immediately report a lost, stolen or compromised device to the City's IT Division. The City reserves the right to remotely wipe a lost or stolen device.

4.7 Work Rules. The following work rules apply to BYOD users:

(a) *Nonexempt BYOD Users*: Unless authorized by their supervisors, users who are classified as nonexempt employees (*i.e.*, employees who are entitled to receive overtime pay) may not use their devices to perform City-related work outside their work hours unless authorized by a supervisor. They should not be regularly reviewing and responding to City emails or texts, for example. Nonexempt users who use their devices to perform City-related work outside of their normally scheduled work hours must track and record their time spent working. Access that is considered "de minimis" (10 minutes or less or insignificant periods of time which are not easily recorded for payroll purposes) does not have to be tracked.

(b) *EEO and Anti-Harassment*: The City's equal employment opportunity policy and its policies prohibiting unlawful discrimination, retaliation and harassment apply to the use of any device. Employees who violate these policies through the use of a device are subject to discipline, including discharge. The City reserves the right to monitor City network usage to ensure compliance with these policies.

(c) *Record Retention*: City data on a device is subject to the same records retention requirements as other City records. Users are required to comply with those requirements.

(d) *Driving*: An Employee is prohibited from using a device for purposes of performing his/her duties on behalf of the City if the employee is driving, even if the device is in "hands-free" mode.

4.8 Costs. The use of a personal device is voluntary. The City will not pay or reimburse the user for the device or for any monthly voice/data charges or for the loss of, or damage to, the device.

4.9 Compliance with Legal Process: By using their personal mobile device to access the City network, the user understands that it becomes possible a court order, subpoena or search

warrant may compel the user to cooperate with a civil or criminal court proceeding and surrender their device temporarily for forensic imaging.

5.0 Discipline:

Violations of this policy will subject the employee to discipline, including discharge, as determined by the Director of Human Resources and the City Manager.

6.0 Contact for Additional Information:

Employees and other BYOD users with questions about this policy should contact the Assistant Director IT Division or the Director of Human Resources.

7.0 Distribution:

Employee Information Site, www.citylf.org.

Robert R. Kiely, Jr.
City Manager

Created 5/2014
Rev. 5/2017