



# Administrative Regulations

Number AR8-37  
Issue 1

**Subject: Employee-Owned Mobile Device/City Email Synchronization Policy**

This Regulation consists of the attached "Employee-Owned Mobile Device/City Email Synchronization Policy" as prepared by the Technology and Innovation Department.

APPROVED:

\_\_\_\_\_  
CITY MANAGER

\_\_\_\_\_  
DATE

ATTACHMENT



**City of Long Beach**  
**Technology & Innovation**  
**Department**

**Employee-Owned Mobile Device / City Email**  
**Synchronization Policy**

**EMPLOYEE-OWNED MOBILE DEVICE/CITY EMAIL SYNCHRONIZATION POLICY**

The City of Long Beach recognizes the importance of employee-owned mobile devices (smartphones, cell phones, etc.) to access City technology resources. The purpose of this policy is to establish standards for accessing City technology resources on employee-owned mobile devices, and to clarify City and employee expectations and responsibilities.

To ensure compliance with the Fair Labor Standards Act (FLSA), the Department of Human Resources will review and approve all requests for employees to access or synchronize City E- Mail on employee-owned mobile devices. Non-management employees who have access to the e-mail system (including texts or any other type of messaging) from any employee-owned mobile device while off-duty shall not perform any City related work (check or respond to work related emails and texts) unless directed and approved by the employee's supervisor in advance.

Nothing in this policy shall be construed as requiring the City to provide any technical resources, assistance, or compensation in support of any employee-owned mobile device, except as described in City Responsibilities.

Employees who elect to utilize an employee-owned mobile device for conducting City business must sign the Employee Acknowledgement Form and Release of Liability at the bottom of this policy.

\*Note: The City does provide employees with a City-issued mobile device, contingent upon Department Head and Department of Human Resources approval.

**Item 1. City Responsibilities**

- Perform initial City email synchronization on employee's personal mobile device.
- The City reserves the right to deny email synchronization with an employee-owned mobile device if it requires that additional City resources be expended to fulfill the request.
- The City assumes no liability for employee-owned mobile devices.
- The City will not attempt to troubleshoot or correct any problems with accessing City resources on an employee-owned mobile device. If an employee has difficulty accessing City email on an employee-owned mobile device, City email can be accessed via an internet browser by accessing the Microsoft Office 365 Webmail site.
- The City will not procure applications specifically for an employee-owned mobile device.

## Item 2. Employee Responsibilities

- Procure and maintain an operable employee-owned mobile device with a data plan from a cellular service provider (Verizon Wireless, AT&T Wireless, T-Mobile, Sprint, etc.).
- Prior to procurement, ensure that the mobile device can be configured to receive City email. Not all devices meet the technical and security specifications. Please contact the Technology & Innovation (TID) Help Desk (x6100) to inquire about minimum device requirements.
- Understand any device hardware and/or operating system limitations as it relates to the City's email and calendaring system.
- Work directly with the cellular service provider and/or device manufacturer to troubleshoot and correct any problems with the device and its functionality.
- The device must have a password enabled to ensure protection of City information.
- Notify commercial service provider and the TID Help Desk (X6100) immediately if a device is lost or stolen. This will limit the risk of unauthorized use. The device should only be used by the employee and should not be shared with family and/or friends.
- Provisions contained within the City's Computer Use Policy and Email and Instant Messaging Use and Acceptance Policy apply to work-related emails that are sent via an employee-owned mobile device.
- The employee is responsible for replacement of an employee-owned mobile device and accessories if broken, lost, or stolen.
- The employee is responsible for any and all charges from the cellular service provider.
- Immediately notify TID through a Service Request if/when the email synchronization is no longer needed.
- Non-management employees who have access to the e-mail system (including texts or any other type of messaging) from any employee-owned device shall not perform any City related work (check or respond to work related emails and texts) while off-duty unless directed and approved by the employee's supervisor in advance.
- Email sent or received via a City email account or any calendar entry placed on Microsoft Office 365 may be considered a public record and may be discoverable even if it was transmitted via a personal mobile device.

## Item 3. Security

The security of City information is of the utmost importance and it is the responsibility of the employee to ensure the employee-owned device is secure. When possible, the employee should initiate a remote "wipe" to erase the contents of the mobile device when it is lost or stolen. The remote "wipe" function erases the contents of the mobile device, including, but not limited to, City email. Personal information transmitted via Microsoft Office 365 or stored on the City's Microsoft Office 365 server may also be erased. The City will not be liable for the loss of any personal data.

Additionally, it is a requirement of this policy that the employee-owned mobile device have the password protection function enabled on the device. City email synchronization will not occur without the password protection function being enabled. It is critical that employees refrain from

putting any confidential, proprietary, or other City information on the device (aside from the City email, calendar, and contacts functions of Microsoft Outlook).

**Item 4. Employee Acknowledgement Form and Release of Liability**

I have read and understand the Employee and City Responsibilities. I further understand that failure to comply with the policy could result in my employee-owned mobile device/City email synchronization privileges being revoked and possible disciplinary action. I release the City, its officers, agents, and employees from any and all claims, causes of action, rights, expenses, costs, losses, and damages arising out of any acts or omissions of the City, its officers, agents, or employees in connection with the synchronization, troubleshooting, maintenance, licensing or protection of Microsoft Office 365 on my personal mobile device.

\_\_\_\_\_

**Type and Model of Smartphone Device**

\_\_\_\_\_  
**Employee Acknowledgement/Signature**

\_\_\_\_\_  
**Employee Classification/Title**

\_\_\_\_\_  
**Print Employee Name**

\_\_\_\_\_  
**Date**

**\*Please ensure that this acknowledgement form accompanies the TID Service Request that seeks the City email synchronization.**