





Interoffice Memorandum

July 20, 2017

TO: Mayor Teresa Jacobs
-AND-
Board of County Commissioners

FROM: Rafael Mena, Chief Information Officer
Information Systems & Services Division 

THRU: Rich Steiner, Enterprise IT Supervisor, Radio Services
Information Systems & Services Division 

SUBJECT: Approval of Memorandum of Understanding Orange County
Intergovernmental Radio System Encryption Key

This Memorandum of Understanding (MOU) is structured as a unilateral agreement allowing Orange County public safety agencies access to the Orange County Intergovernmental Radio System. There will be no cost to Orange County since there is no additional equipment involved with this agreement. The MOU will establish parameters for use of a common encryption key for the public safety radios operating on the system.

ACTION REQUESTED: Approval of Memorandum of Understanding Orange County Intergovernmental Radio System Encryption Key by and between the Orange County Sheriff's Office, the City of Apopka, the City of Belle Isle, the Town of Eatonville, the City of Edgewood, the City of Maitland, the Town of Oakland, the City of Ocoee, the City of Orlando, the University of Central Florida, the Town of Windermere, the City of Winter Garden, the City of Winter Park, Orange County Government, and Orange County School Police for public safety radios operating on the Orange County Intergovernmental Radio System at no cost to Orange County.

RM/RS/ri

c: Eric Gassman, Chief Accountability Officer, Office of Accountability

BCC Mtg. Date: Aug. 1, 2017

MEMORANDUM OF UNDERSTANDING

Orange County Intergovernmental Radio System Encryption Key

THIS AGREEMENT, made this _____ day of **AUG 01 2017**, 2017, by and between the Orange County Sheriff's Office, hereinafter referred to as the "Sheriff;" the City of Apopka, hereinafter referred to as "Apopka;" the City of Belle Isle, hereinafter referred to as "Belle Isle;" the Town of Eatonville, hereinafter referred to as "Eatonville;" the City of Edgewood, hereinafter referred to as "Edgewood;" the City of Maitland, hereinafter referred to as "Maitland;" the Town of Oakland, hereinafter referred to as "Oakland;" the City of Ocoee, hereinafter referred to as "Ocoee;" the City of Orlando, hereinafter referred to as "Orlando;" the University of Central Florida, hereinafter referred to as "UCF;" the Town of Windermere, hereinafter referred to as "Windermere;" the City of Winter Garden, hereinafter referred to as "Winter Garden;" the City of Winter Park, hereinafter referred to as "Winter Park;" Orange County Government, hereinafter referred to as "Orange County;" and Orange County School Police, hereinafter referred to as "School Police" agree as follows:

WHEREAS; the parties to this agreement are all governmental public safety agencies who share common public safety radio systems, and

WHEREAS; certain communications and information transmitted over said radios contain confidential and emergency information not subject to public disclosure, and

WHEREAS; the parties believe that it is necessary to ensure the confidentiality and security of radio transmissions made by their public safety agencies.

NOW THEREFORE; the parties agree to the establishment of parameters for use of a common encryption key for all public safety radios operating on the Orange County Intergovernmental Radio System.

1. Term

The term of this agreement shall commence on the _____ day of **AUG 01 2017**, 2017 and shall be automatically renewable on a year-to-year basis.

2. Termination

Parties may withdraw from this agreement upon sixty (60) days prior written notice to all other participants. The parties individually agree that in the event that they withdraw from this agreement, any encryption information previously provided to them including the encryption key will remain confidential.


3. Policy

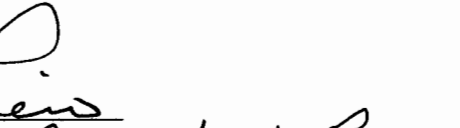
The user agencies operating on the Orange County Intergovernmental Radio System hereinafter referred to as the "Radio System" will:

1. Agree to utilize the same encryption key for all public safety radios.
2. Agree to keep the encryption key in a secure location and to take every precaution to keep the key secret.
3. Immediately notify the Orange County Sheriff's Office in the event they have reason to believe that the confidentiality of the encryption key has been compromised.
4. Agree not to change the encryption key used for the Radio System without coordinating that change with all of the other signatories of this Agreement.
5. Agree not to program the encryption key into any non-public safety radio.
6. Agree not to release the encryption key to any other user or entity not listed as a signatory to this agreement without the express prior written consent of all of the signatories.
7. Not provide encrypted radios for use by non-public safety personnel.
8. Agree to periodically change the encryption key for the Radio System in concert with the other signatories.
9. Agree not to release the encryption key to any agency outside Orange County, Florida, unless law enforcement agencies require access for mutual aid. (Examples: Task Force, MBI, etc.)

4. Amendments

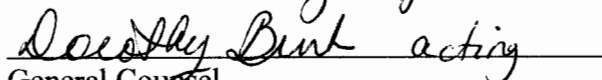
This Agreement shall not be amended except in writing and executed by the parties.


Jerry L. Demings
as Sheriff of Orange County, Florida

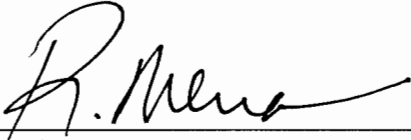

Rinaldo L. Rivero
Undersheriff,
Acting Sheriff

Date: 7/20/17

FOR USE AND RELIANCE ONLY BY THE
SHERIFF OF ORANGE COUNTY, FLORIDA.
APPROVED AS TO FORM AND LEGALITY
THIS 20 DAY OF July, 2017.


General Counsel

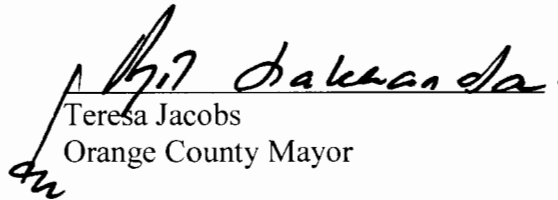
ORANGE COUNTY GOVERNMENT



Rafael Mena
Chief Information Officer
Information Systems & Services

APPROVED:
ORANGE COUNTY, FLORIDA

ATTEST: 


Teresa Jacobs
Orange County Mayor

APPROVED BY THE BOARD OF COUNTY
COMMISSIONERS FOR ORANGE COUNTY,
FLORIDA, AT A MEETING HELD ON
AUG 01 2017

UNDER AGENDA NO. _____.

FOR USE AND RELIANCE ONLY
BY ORANGE COUNTY,
FLORIDA. APPROVED AS TO
FORM AND LEGALITY THIS
____ DAY OF _____, 2017.

County Attorney