Title: **Managing Encryption**

Index: 204-A

Effective Date:

Revision/Date: 0

Author: Rick Brown, PCWIN Wireless Services

Owner: Operations Working Group (OWG)

1. **Purpose**
    a. The Encryption Management guidelines set forth in this procedure are intended to ensure the proper security, management, generation, distribution, use, storage, and destruction of Pima County Wireless Integrated Network (PCWIN) encryption key materials.

2. **Background**
    a. PCWIN radio communications may contain sensitive and vital information relative to public safety activities. Disclosure or modification of this information could adversely impact public safety operations and pose a threat to the safety of public safety officials and citizens. PCWIN has recognized the need for protecting sensitive radio transmissions and has equipped the PCWIN system with AES encryption capabilities and multi-key Over-The Air Rekeying (OTAR).
    b. The generation of PCWIN encryption keys and distribution of those keys to subscribers in a synchronized fashion is a complex process critical for encrypted radio transmissions. There are inherent risks and vulnerabilities to public safety personnel if proper key management processes are not followed. PCWIN can significantly mitigate these risks and vulnerabilities by establishing standard key management processes.
    c. Each PCWIN encryption key is associated with a system-wide key reference, referred to as a Common Key Reference (CKR). The same encryption key is referenced by the same CKR in every secure component, and allows key management in a device independent manner. CKRs are assigned to talkgroups and multi-groups.

3. **Procedure Statement**
    a. All PCWIN members with encrypted talkgroups will designate an encryption Common Key Reference for their encrypted talkgroups. The CKR can be assigned to a single or multiple talkgroups.
    b. Each agency who owns encrypted talkgroups shall appoint an Encryption Key Coordinator who can determine the control and authorization of the encryption keys associated with agency owned talkgroups.
        i. Each CKR will have a single designated Encryption Key Coordinator that is assigned by talkgroup owner.
            1. All authorizations for use and distribution of the encryption keys will be made in writing by the approved Encryption Key Coordinator.

2. The Encryption Key Coordinator will have the authority to request modification of any assignment of the CKR.

c. The PCWIN Executive Director will maintain an encryption key map showing current assignments and authorizations, and a list of CKR. This information will be distributed periodically to the Encryption Key Coordinator for validation. Subsequent changes to the current encryption key map and list of owners will be by notification of exception.

d. Key Generation
    i. PCWIN encryption keys will be generated by the Pima County Network Managing Member using the automatic key generation capabilities of the Key Management Facility (KMF).
    ii. New encryption keys will be generated using 256 bit Advanced Encryption Standard (AES).
    iii. The targeted crypto-period (i.e. the time period during which any given key material will be active) will be 12 months, or as needed.
    iv. Ranges for the CKRs are maintained by the Network Managing Member.

e. Key Distribution
    i. Member agencies are not authorized to own a PCWIN provisioned Key Variable Loader (KVL) unless expressly provided authorization through the OWG.
    ii. Authorized KVLs will contain the Universal Key Encryption Key (UKEK), also known as the “Shop Key”, and other keys approved by the Key Owner(s).
    iii. PCWIN subscribers which require encryption must have the Shop Key loaded using an authorized KVL.
    iv. All encryption keys for subscribers will be updated via the KMF only.
    v. Manual loading of Universal Key Encryption Key (UKEK) via a KVL into any subscriber is not authorized without the approval of the OWG.
    vi. Console Key Loading
        1. Rekeying of talkgroups programmed into subscriber units will prompt a contemporaneous rekeying of those consoles and backup control stations with authorized encrypted access to the same talkgroups.
    vii. Encryption keys will be changed at predetermined times as defined by the Encryption Key Coordinator(s). Destruction of active key material contained in a subscriber will be accomplished by zeroizing the key set in the subscriber via the KMF, KVL, or manual operation if available.
    viii. If a subscriber is experiencing encryption related issues, it may have missed critical updates. The user may perform a subscriber initiated “Rekey” request. If that does not correct the problem, contact the PCWIN Wireless Services office.

f. Key Material Distribution

i. Requests for distribution of Member owned key material to be used in nonmember KVL and KMFs must be made in writing (letter or email) by the Key Owner, and sent to the PCWIN Executive Director.
ii. It will be the responsibility of the PCWIN Executive Director to present the OWG a written request for distribution of Universal Key Encryption Key (UKEK) to be used in a non-member KVL or KMF to the OWG for approval.
    a. The agency making the request must include the following: Purpose for the request, number of subscribers needing access, key material requested (i.e., Universal Key Encryption Key (UKEK), talkgroup CKR(s)) and the name and contact information for the non-member agency.
    b. Distribution of encryption keys will be by physical exchange of the key material directly from the KMF to the KVL device(s).
    c. The receiving agency must have an IGA, MOU, or other binding document granting Pima County (PCWIN Wireless Services) authority to program and bill for programming services.
iii. Universal Key Encryption Key (UKEK) or the Shop Keys will not be transferred by direct KVL to KVL connection without the approval of the Pima County Network Managing Member.
iv. Agencies must provide a report of all subscribers containing any PCWIN agency owned key material within three (3) business days upon request by the PCWIN Executive Director
v. It will be the responsibility of the non-member agency to obtain new key material in the event of an encryption key set change.
vi. If approved, use of PCWIN key material in a non-member KVL and/or KMF is subject to time limitations and authorizations may be reviewed on an annual regular basis.

g. Encryption Materials
    i. The PCWIN encryption database will be backed up and stored in a secure onsite and offsite location by the Pima County Network Managing Member. The PCWIN encryption database will be stored in encrypted format.
    ii. If the integrity of the PCWIN encryption database is compromised, all PCWIN key material will be immediately changed

h. Pima County Network Managing Member will provide encryption services during normal business hours, Monday through Friday, 7:00 am to 5:00 pm, excluding Pima County defined holidays. Any requests received after hours will be processed according to the timelines outlined in this policy. Any after hour support requests will be evaluated on a case-by-case basis and will only be considered in exigent circumstances

i. A minimum of three (3) business days lead time is required for all encryption requests, unless special circumstances exist. Larger projects may require a longer lead time

i. Authorized KVL Holder Responsibilities
    i. Ensuring KVL devices will be physically secured at all times when not in use.
    ii. Responsible for loading of the initial UKEK ("Shop Key") or authorized encryption keys into all PCWIN subscribers requiring secure capabilities.
    iii. Verifies that the OTAR ID matches the subscriber ID before loading encryption keys.
    iv. Immediately reports any known or suspected incident involving compromised key material to the Pima County Network Managing Member, who in turn notify PCWIN Director and OWG.

j. PCWIN Participating Agencies
    i. Maintain inventory control of secure subscribers.
    ii. Designate individual(s) in the agency to act as the Encryption Key Coordinator.
        1. Each secure key will have a single Member owner.
        2. The Member must identify a primary point of contact regarding the Member's encryption key administration. An alternate point of contact may be identified to act in the absence of the Encryption Key Coordinator.
        3. Responsible for implementing a training program for agency personnel relative to proper use of subscribers containing encryption keys.

k. End Users (Subscribers)
    i. Protects subscribers with encryption keys in all situations.
    ii. Immediately notifies the appropriate personnel, as determined by their agency, concerning lost, stolen, and/or compromised subscribers.
    iii. Notifies proper personnel immediately of any known or suspected incident involving keying material and submits incident reports to the appropriate personnel as determined by agency policies and procedures.
    iv. Responsible for requesting encryption keys, through the Pima County Network Managing Member.
    v. Notify the PCWIN Executive Director immediately regarding matters relative to lost or stolen subscribers, compromised key materials, and other encryption related incidents as appropriate.
    vi. Responsible for ensuring users of the Key Owner's key materials are aware of the subscriber responsibilities set forth in this procedure.

l. PCWIN Dispatch Supervisors or other designated agency personnel
    i. Requests for Creation of CKRs must be made in writing using CommSHOP and sent to the Pima County Network Managing Member. This request must include CKR number, CKR name, and Key Owner information.

ii. Addition or Changes to Subscribers in the KMF: All requests for the addition of new subscriber IDs or any encryption changes requested to existing IDs or names must be made using CommShop. Requests for encryption permissions will be the responsibility of the requesting agency to secure from each Key Owner affected. Additions or change requests need to be sent to the Pima County Network Managing Member for processing.

iii. Lost, Stolen or Compromised Subscribers

1. Upon notification of a lost, stolen, or compromised subscriber, the Pima County Network Managing Member will set the subscriber for key deletion.

2. Once the subscriber keys are successfully deleted, the PCWIN Network Managing Member and the affected agency will be notified so an inhibit command may be sent. If the subscriber is not recovered after one year, the subscriber record will be deleted from the KMF and notification will be sent to the agency and PCWIN Network Operations.

4. Applies to

a. All users of the 800 MHZ Digitally trunked radio system's secure capabilities

5. Supporting Rules

a. None

6. Conditions for Exemption or Waiver

a. None