REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES	No. **S-02.10**
Subject: **Encryption Management Guidelines Policy**	**Revised: 03/2024** **Prior Rev:** **07/2023** **09/2019** **07/2010**

1.0 Purpose

1.1. The Encryption Management guidelines set forth in this policy are intended to ensure the security, management, generation, distribution, use, storage, and destruction of Regional Wireless Cooperative (RWC) encryption key materials.

2.0 Owner

2.1. RWC Operations Working Group (OWG).

3.0 Applies To

3.1. All RWC Members, Interoperability Participants, and entities having subscribers authorized to use the secure operational capabilities of the RWC.

4.0 Background

4.1. RWC communications often contain sensitive and vital information relative to law enforcement and other public safety related 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. The RWC has recognized the need for protected radio transmissions and has equipped the network with encryption capabilities that provide the required level of protection.

4.2. The generation of RWC encryption keys and distribution of those keys to subscribers in a synchronized fashion is a complex process that is critical to the encryption of radio transmissions. There are inherent risks and vulnerabilities to public safety personnel if proper key management processes are not followed. The RWC can significantly mitigate these risks and vulnerabilities by establishing standard key management processes.

4.3. Each RWC 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.

5.0 Policy Statement

5.1. The Managing Member(s) shall provide key management services, including generation, distribution, storage, destruction, and maintenance of key materials. Individual Members may be required to update key materials in Subscriber Units as directed by the RWC. The RWC may designate other agencies, such as Federal agencies, to provide key management services in special circumstances.

6.0 Supporting Rules

6.1. The Encryption Services Manager (ESM) will administer the RWC encryption management program for RWC Members.

6.2. RWC Members using encryption will designate an Encryption Key Owner for the control and authorization of the encryption keys associated with Member owned talkgroups.

6.2.1. Each CKR will have a single designated Key Owner that is assigned by talkgroup owner.

6.2.2. Interoperability Encryption Keys are owned by the OWG.

6.2.3. All authorizations for use, distribution, or modification of the encryption keys will be made in writing by the approved Key Owner using the RWC workbook.

6.2.4. PSAP Encryption keys are owned by the ESM.

6.3. The Encryption Services Manager will maintain an encryption key map showing current assignments and authorizations, and a list of CKR Owners. This information will be distributed periodically to the Encryption Key Owners for validation.

6.4. Key Generation

6.4.1. RWC encryption keys will be generated by the Encryption Services Manager using the automatic key generation capabilities of the Key Management Facility (KMF).

6.4.2. RWC encryption keys will be generated using 256-bit Advanced Encryption Standard (AES).

6.4.3. The active key material will be changed on a periodic basis, not to exceed 24 months.

6.4.3.1. Inactive key materials role is for archiving purposes to assist the transition to new active keys.

6.4.4. Ranges for the CKRs are maintained by the Encryption Services Manager.

6.4.5. Shop key material will be changed within a 48-month period and coordinated with the active key generation change cycles.

6.5. Key Distribution

6.5.1. Member agencies are required to own or have access to a Member owned RWC provisioned generic Key Fill Device (KFD) or specific Key Fill Devices such as the Motorola KMF.

6.5.2. KFDs owned by other entities and provisioned by the RWC must be formally authorized by the OWG with input derived from the Encryption Services Manager.

6.5.3. Authorized KFDs may contain a Universal Key Encryption Key (UKEK).

6.5.4. The RWC does not permit contractor owned Key Fill Devices (KFDs).

6.5.4.1. Contractors shall coordinate with the Encryption Office for all encryption services.

6.5.5. The RWC requires that all encryption keys for subscribers be sent or updated via the KMF only, through the Over the Air Rekeying (OTAR) process.

6.5.6. Manual loading of CKR 1, CKR 200 via a KFD into any subscriber is not authorized without the approval of the OWG.

6.5.7. Console Key Loading

6.5.7.1. Primary agency dispatch consoles will require the use of Over the Ethernet Keying (OTEK) for loading of a UKEK using an authorized KFD or other secure media.

6.5.7.1.1. An encrypted password protected portable flash drive would be an example of secure media.

6.5.7.2. Secondary Agency dispatch consoles that do not support OTEK must have keys manually loaded via KFD or other secure media by a responsible Member agency.

6.6. Key Material Distribution (KFD/KMF)

6.6.1. Agency requests for distribution of Member owned key material to be used in non-member KFD and KMFs must be made in writing (letter or email) by the Key Owner and sent to the Encryption Services Manager.

6.6.2. Distribution of encryption keys will be by physical exchange of the key material directly from the KMF to the KFD or other secure media. RWC keys shall not be transferred by direct KFD to KFD connection.

6.6.3. Agencies must provide a report of all subscribers containing any OWG owned key material within three (3) business days upon request by the RWC.

6.6.4. It will be the responsibility of the non-member agency to obtain new key material in the event of an encryption key set change.

6.7. Encryption Materials

6.7.1. The RWC encryption database will be backed up and stored onsite in the Encryption Services Office, as well as offsite as designated by the Encryption Manager.

6.7.2. The RWC encryption database will be stored in encrypted format.

6.7.3. If the integrity of the RWC encryption database is compromised, all RWC key material will be immediately changed.

6.8. Auditing

6.8.1. Any KFD, portable, or mobile radio containing encryption keys must be zeroed when decommissioning or removing from service.

6.8.2. Any KFD or UKEK (containing encryption material) must be reviewed annually by the Encryption Services Manager or their delegate.

6.8.3. Any removable media should be secure through encryption and password protection mechanisms. Devices such as USB drives or portable drives that cannot meet this criteria should not be used.

7.0 Responsibilities

7.1. The Encryption Services Manager will provide encryption services during normal business hours, Monday through Friday, 8:00 am to 4:00 pm, excluding defined holidays. All encryption related requests should be sent to RWC.Encryption.ppd@phoenix.gov. 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.

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

7.2. Encryption Services Manager

7.2.1. Equates to the Administrative Managing Member Police Network Manager and Oversees Encryption Services Operator(s). A delegate may perform these duties in the event of the manager's absence.

7.2.2. Shall coordinate with the RWC to ensure the Key owners are included in the Compromised Radios Email group and review the list annually.

7.2.3. Performs key management functions on a day-to-day basis.

7.2.4. Protects keying materials and limits access to individuals with a valid need-to-know.

7.2.5. Configures security features of key management system components in accordance with RWC policies.

7.2.6. Maintains required RWC encryption key workbooks and related documentation for a period of 24 months.

7.2.7. Performs periodic backup of KMF databases.

7.2.8. Reports any known or suspected incident involving keying material to the OWG.

7.2.9. Creates and loads keys into KFDs or other secure media.

7.2.10. Coordinates with RWC members relative to the daily operational aspects of RWC encryption.

7.2.11. Responsible for receiving and investigating any encryption-related incidents, including oversight of corrective actions related to compromised subscribers containing encryption keys.

7.2.12. Zeroizes subscribers from the KMF that have become compromised.

7.2.13. Authorizes the establishment, modification, and closure of system accounts for the key management facility.

7.2.14. Provides administrative guidance on the implementation of RWC key management activities.

7.2.15. Assigns all CKR numbers as part of the talkgroup approval process.

7.2.16. Ensures that encryption reports are generated monthly and distributed.

7.2.17. Ensures that currency reports are generated quarterly and distributed.

7.2.18. Ensures completion of annual KFD audit.

7.3. RWC Executive Director is responsible for facilitating requests from outside agencies for KFD or other secure media access to RWC key material and presenting the requests to the OWG for approval.

7.4. Authorized KFD Owner Responsibilities

7.4.1. Encryption key material must be physically secured at all times when not in use.

7.4.2. Loading of the initial UKEK or authorized encryption keys into RWC subscriber devices requiring secure capabilities.

7.4.3. Verifies that the Radio Set Identifier (OTAR ID) matches the subscriber ID before loading encryption keys.

7.4.4. Immediately reports any known or suspected incident involving compromised key material via the RWC notification process.

7.5. RWC Participating Agencies

7.5.1. Maintain inventory control of secure subscribers.

7.5.2. Designate individual(s) in the agency to act as the Key Owner.

7.5.2.1. Each secure key will have a single owner.

7.5.2.2. The Agency may delegate a temporary alternate Key Owner to act in the absence of the primary Key Owner.

7.5.3. Load and maintain agency owned KFDs or other secure media.

7.5.4. Any agency utilizing encryption capable consoles must have access to their own KFD, other secure media, or arrangements are required to be made with another Member to provide this service.

7.5.5. Responsible for reporting lost or compromised radios to the RWC using the established distribution list (see RWC Compromised Radio Procedure).

7.6. Key Owners

7.6.1. Responsible for authorizing subscriber encryption through the Encryption Services Manager.

7.6.2. Shall notify the Encryption Manager of any changes in the Key owner.

8.0 Encryption Management Process

8.1. Requests for Creation of CKRs

8.1.1. CKR creation requests must be made in writing (letter or email) and sent to the Encryption Services Manager. This request must include CKR number, CKR name, and Key Owner information.

8.2. Addition or Changes to Subscribers in the KMF

8.3. All requests for the addition of new subscriber IDs or any encryption changes requested to existing IDs or names must be made using the approved RWC workbook. 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 Encryption Services Manager for processing.

9.0 Conditions for Exemption or Waiver

9.1. As provided in the Waiver or Exception Policy.

10.0 Applicable Policies and/or Procedures

10.1. As listed at www.rwcaz.org.