REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES	 **No.** **S-03.12**
Subject: **Compromised Radio Procedure**	**Revised: 11/2025** **Prior Rev: 08/2021**

1.0 Purpose

1.1 Define a notification procedure for a compromised subscriber unit.

2.0 Owner

2.1 Regional Wireless Cooperative (RWC) Operations Working Group (OWG).

3.0 Applies To

3.1 All Members, Interoperability Participants and entities otherwise having subscribers using the RWC Network.

4.0 Background

4.1 Compromised subscriber units may be used maliciously to interfere with public safety and service operations.

5.0 Policy Statement

5.1 Compromised subscriber units will be reported as soon as practicable.

6.0 Supporting Rules

6.1 Once notification of a compromised subscriber unit is received, the agency designee will regroup the unit to a predetermined talkgroup, if possible.

6.1.1 There will be one talkgroup designated for the entire RWC.

6.1.2 The talkgroup will not have emergency alert capabilities.

6.1.3 The talkgroup may be recorded and monitored by any RWC dispatch facility.

6.2 The subscriber until will be zeroized as soon as possible by RWC Encryption Services staff.

6.2.1 Subscriber units not managed by RWC Encryption Services cannot be zeroized.

6.3 The Administrative Manager will maintain a record of all radios reported compromised.

6.3.1 After a period of one year the radio ID will be removed from the system.

6.3.2 The radio ID will not be reissued.

7.0 Responsibilities

7.1 Reporting agencies with access to Radio Control Manager (RCM) will manage any compromised radios owned by that agency, as described in Section 6.

7.1.1 Reporting agencies without access to RCM will contact the Network Operations Center (NOC) via the rwc.lost@phoenix.gov mailbox to facilitate the process during business hours Monday through Friday, 8 a.m. to 4 p.m.

7.1.2 Compromised radios disrupting operations will be handled by the RWC Network Administrator.

7.2 Compromised radios will be reported to the RWC using the established distribution list.

7.3 The report will contain as much of the following information as possible:

7.3.1 Make/Model/Serial Number.

7.3.2 Approximate location of occurrence.

7.3.3 Approximate date/time of occurrence.

7.3.4 Subscriber radio ID.

7.3.5 Individual agency asset number/tag where applicable.

7.3.6 If the subscriber unit contains encryption keys.

7.3.7 Police report where applicable.

7.3.8 Reporting party contact information.

7.4 If the subscriber unit is recovered, reporting agencies will notify the RWC using the established distribution list.

8.0 Conditions for Exemption or Waiver

8.1 As provided in the Waiver or Exception Policy.

9.0 Applicable Policies and/or Procedures

9.1 As listed at www.rwcaz.org.