REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES	Regional Wireless Cooperative
	No. S-05.11
Subject: Radio Site Security Procedure	Effective Date 3/23/11 Rev: 02/11/15

1.0 Purpose

1.1. The purpose of this procedure is to define radio site security related to communications facilities owned and/or operated by the Regional Wireless Cooperative (RWC).

2.0 Owner

2.1. RWC Operational Working Group (OWG).

3.0 Applies To

3.1. RWC facility owners and service providers with access to RWC radio communications facilities.

4.0 Background

4.1 The RWC operates radio communications facilities that provide wireless communication in support of public safety and public service on a regional basis. These locations contain sensitive electronic equipment requiring monitoring, protection and access restrictions.

5.0 Policy Statement

5.1 Members who own wireless communications facilities that are utilized by the RWC shall establish and maintain site access security procedures for remote communications facilities. Members will also provide physical security protection to RWC Network equipment and facilities through the use of barriers, facility entry control systems and monitoring equipment.

5.2 All requests for personnel requiring access and/or security badges shall be made in writing to the Member who owns the facility as appropriate. Personnel may be subject to background checks depending on the security level and policies for critical infrastructure.

5.3 In the event of a security threat (fire, unauthorized entry, vandalism, etc.), on site individuals will retreat to a safe location, and as soon as practical, dial 911 in response to the threat. They shall also notify RWC Operations Center of the event and potential impact to RWC Systems.

6.0 Supporting Rules

6.1. All security incidents or entry/access violations shall be reported to RWC Operations Center.

6.2. Occupants and/or workers at secure facilities must have appropriate badges/or access authorization material displayed in plain view at all times. If access has not been granted then an authorized escort must be present at all times.

6.3. Sharing of access cards is not permitted.

7.0 Responsibilities

7.1. Members who own and operate communications facilities on behalf of the RWC will ensure that personnel requiring access are properly trained and aware of the facility access security policies.

7.2. Members who own and operate communications facilities on behalf of the RWC will ensure these critical facilities are properly secured and protected.

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