
AFRRCS Agency Handbook

Section: Policies and Procedures Documents

Contents

1. Agencies
 - a. Agency Positions, Training and Security
2. Permitted Radios
 - a. Permitted Radio Policy
3. Radio Programming
 - a. Programming Key Policy
4. Talkgroups
 - a. Talkgroups
 - b. Coverage Classes
 - c. Talkgroup Naming Policy
 - d. Talkgroup priority
 - e. Patching Policy
 - f. Unconfirmed Talkgroups
 - g. Agency Interoperability Contact
5. Voice is Primary Service
 - a. PTT Voice is Primary Service
 - b. Data Primary Service
6. Trunking Features
 - a. Trunking Features
7. Encryption
 - a. AES and KMF Vendor
 - b. Link Layer Authentication
8. Over the Air Updates
 - a. Over the Air Rekeying
 - b. Over the Air Programming
9. Connectivity
 - a. Agency Network Connectivity Policy
10. Site on Wheels and Radio Cache Deployment
 - a. Provincial Emergency Support and Deployed Operations

HANDBOOK REVISION HISTORY

Version	Date	Modified By	Section Revised
0.1	July 22, 2015	BS	First Draft
1.0	January 5, 2016	BS	First version, removed drafts.
2.0	March 22, 2016	BS	Added new and amended policies approved by AFRRCS Governance; Dispatch Center Connectivity (Amended to v02), Patching (new), Programming Key (new), Talkgroups (amended to v02), Unconfirmed Talkgroups (new)
3.0	June 27, 2016	BS	Added new and amended policies approved by AFRRCS Governance; AES and KMF Vendor v02, Agency Positions Training and Security v02, Coverage Classes v02, OTAP v02, OTAR v02, PTT Voice Primary Service (new), Talkgroup Naming Conventions v02, Talkgroup Priorities v02, Trunking Features (new)
4.0	October 25, 2016	KC	Added new and amended policies approved by AFRRCS Governance: <ul style="list-style-type: none"> • Agency Interoperability Contact (new) • Call Availability (combined the Talkgroup Priority, and Unconfirmed Talkgroup Policies with a new call timer policy) • Provincial Emergency Support and Deployed Operations v02 (replaced the Site on Wheels Deployment policy) • Talkgroup Naming Conventions (updated) • Talkgroups (updated)
5.0	July 09, 2018	CB	Added new and amended policies approved by or presented to AFRRCS Governance: <ul style="list-style-type: none"> • Permitted Radio Policy (Updated) • Talkgroups (Updated) • Coverage Classes (Updated) • PTT Voice is Primary Service (Updated) • Data Primary Service (New) • Trunking Features (Updated) • AES and KMF Vendor • Link Layer Authentication (Added) • Over the Air Keying (Updated) • Over the Air Programming (Updated) • Agency Network Connectivity Policy (Updated) • Provincial Emergency Support and Deployed Operations(Updated) • Permitted Radio List (Updated) • Transformation Forms (New) • Legacy System Interoperability (New) • Lessons Learned Template (New)

AFRRCS Policies and Procedures for Interoperability

Section: Agency Positions, Training, and Security
Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	January 26, 2015	BS	First draft agency position & training requirements policy
0.2	February 27, 2015	BS	Update based on February WG meeting
0.3	March 9, 2015	KC	Formatted for final approval
1.0	June 23, 2015		Approved by AFRRCS Governance Council
1.1	October 26, 2015	BS	Amend training requirements for Technical Administrator
1.2	April 5, 2016	KC	Formatted for annual policy review
1.3	June 2, 2016	KC	Annual review approved by IS Council
2.0	June 21, 2016		Annual review approved by Governance

Contents

Agency Position, Training and Security Policy..... 7

1.1 Agency Administrator..... 7

1.2 Technical Administrator 7

1.3 Agency Trusted Technician..... 8

1.4 Radio End User 8

1.5 Agency Console Operator 8

1.6 Agency Crypto Officer 9

1.7 Effective Date 9

Appendix 10

2.1 Course Descriptions..... 10

Section

1

Agency Position, Training and Security Policy

Each agency is responsible for the duties defined in each of the following positions. Crypto Officer and Console Operator position may not be required for each agency. Minimum training standards are listed for each position. An Agency Administrator and Technical Administrator must be named for each agency. The Administrator position:

- Must have signing authority for the Agency
- Cannot be contracted to a third party.

All other duties and positions can be contracted to third parties, if the agency so chooses. Individuals may fill more than one position, as long as they adhere to the training and security requirements for each position filled.

1.1 Agency Administrator

- a. Required Background
 - i. Understanding of radio communications usage in agency
 - ii. Management responsibility for agency communications
- b. Responsibilities
 - i. Single point of contact for the agency and the OMS
 - ii. Cannot be contracted out and requires agency signing authority
 - iii. Receives, applies for, delegates agency radio programming dongles
- c. Minimum Training
 - i. AFRRCS Policies & Guidelines course
- d. Minimum Security Level
 - i. Refer to AFRRCS Security Policy
 - ii. Agency standard

1.2 Technical Administrator

- a. Required Background
 - i. Understand P25 terminology, components and operational processes
 - ii. Understand fleet mapping concepts and the AFRRCS implementation of fleet mapping
 - iii. Capable of logging into UAS to access user accounts
 - iv. Concepts of Over the Air Rekeying (OTAR)
- b. Responsibilities
 - i. Maintain system databases using the Unified Administration System (UAS)
 - ii. Adding/deleting users
 - iii. Adding/deleting talk groups
 - iv. System monitoring at agency level
 - v. Activity reporting
 - vi. Establish support policy for agency
 - vii. Initiates trouble calls to the OMS
 - viii. Access AFRRCS metrics
 - ix. Manage use of VTI
 - x. Manage and configure voice logger, consoles
 - xi. Contacts other PSAPs directly
- c. Minimum Training
 - i. AFRRCS Policies and Guidelines Course Self-Study
 - ii. 2 day AFRRCS provided Technical Administrator Training course

1.3 Agency Trusted Technician

- a. Required Background
 - i. Working technical knowledge of radios, programming
 - ii. Working technical knowledge of agency communications environment
- b. Responsibilities
 - i. Programs Radio
 - ii. Receives keys from Agency Crypto Officer- Agency directed
 - iii. Manual Key Loading to radios, logging recorders and consoles
 - iv. Radio Repairs
 - v. Mobile installation
 - vi. Retain inventory, inventory management
 - vii. User Training - trains the agency end-user
 - viii. Console installs, programming, updating, Database mgt.
 - ix. Manages and configures voice logger
 - x. Manages and configures consoles for responsible agencies
 - xi. Manages and configures telephones
 - xii. Does not liaise directly with OMS to troubleshoot
 - xiii. Contact other PSAPs directly
- c. Minimum Training
 - i. AFRRCS Policies and Guidelines Course
 - ii. Vendor radio technical training
- d. Minimum Security Level
 - i. Refer to AFRRCS Security Policy
 - ii. Agency minimum

1.4 Radio End User

- a. Understanding Required
 - i. Radio indicators and icons
 - ii. Radio alert tones
 - iii. Make and receive group calls
 - iv. Change groups, change systems
 - v. Declare, receive and clear emergency
 - vi. Place and receive individual calls
 - vii. Return missed individual calls
 - viii. Utilize scanning function
 - ix. Change battery
- b. Minimum Training
 - i. Vendor subscriber radio user course
- c. Minimum Security Level
 - i. Refer to AFRRCS Security Policy
 - ii. Agency minimum

1.5 Agency Console Operator

- a. Required Background
 - i. Console functions
 - ii. Dispatch knowledge
- b. Function Requirements
 - i. Pick and select communication channels
 - ii. Transmit and receive group and individual calls
 - iii. Transmit, receive and clear emergency calls
 - iv. Review call history
 - v. Modify communication modules

- vi. Create, modify and transmit on Patches and Simulselects
- vii. Change console setups
- viii. Use special and enhanced console features
- c. Minimum Training
 - i. Console vendor specific training
- d. Minimum Security Level
 - i. Refer to AFRRCS Security Policy
 - ii. Agency minimum

1.6 Agency Crypto Officer

- a. Required Background
 - i. Understanding of encryption usage in agency
- b. Responsibilities
 - i. Manage accounts
 - ii. Configure crypto networks
 - iii. Rekey talk groups, user and system keys using the Unified Administration System (UAS)
 - iv. Managing encryption Keys through the Key Management Facility (KMF)
- c. Minimum Training
 - i. AFRRCS Policies and Guidelines Course Self-Study
 - ii. 2 day AFRRCS provided Technical Administrator Training course
 - iii. Crypto Officer Course
 - iv. AFRRCS Policies
 - v. Radio vendor course
- d. Minimum Security Level
 - i. Refer to AFRRCS Security Policy
 - ii. Agency standard

1.7 Effective Date

Agency Position and Training policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

Section

2

Appendix

2.1 Course Descriptions

Course	Description	Days	Provider
AFRRCS Policies and Guidelines	One day introductory course to AFRRCS Policies and Guidelines covering material from the Agency Handbook.	1 day	Self-Study
Technical Administration Course	Two day course covering P25 technology and AFRRCS implementation, basic trunking features, fleet mapping, accessing the UAS database, and radio programming	2 days	Provided by AFRRCS
Crypto Officer	This course provides system administrators and managers with the knowledge and skills to manage encryption keys using the Key Management Facility (KMF) product in a P25 ^{IP} network. This includes defining Crypto Officer Administration classes and user privileges; managing Crypto Officer user accounts; configuring crypto nets; and rekeying talk groups, users and system keys using the Unified Administration System (UAS). Completion of the AFRRCS Technical Administrator Course is a prerequisite for the Over the Air Rekeying and Encryption classes.	1 day	Provided by AFRRCS

Whenever possible, courses will be offered within Alberta. AFRRCS does not charge for courses it provides.

AFRRCS Policies and Procedures for Interoperability

Section: Permitted Radio Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	Jan 23, 2015	BS	First draft version Permitted Radio Policy
0.2	March 4, 2015	BS	Final draft from I&S Council
0.3	March 9, 2015	KC	Formatted for approvals
1.0	June, 23, 2015		Approved by AFRRCS Governance with the addition of permitted radio tests into Appendix A
1.1	April 5, 2016	KC	Formatted for annual policy review
1.2	May 19, 2016	BS	Add Aeronautical Category & Tests
1.3	June 2, 2016	KC	Annual Review and aeronautical tests approved by IS Council
2.0	June 21, 2016		Approved by Governance.

Contents

<u>Permitted Radio Policy</u>	Error! Bookmark not defined.
<u>1.1 Permitted Radio Policy</u>	Error! Bookmark not defined.
<u>1.2 Effective Date</u>	Error! Bookmark not defined.
<u>Appendix A – Permitted Radio Tests</u>	Error! Bookmark not defined.
<u>1. Emergency ID and Alarm</u>	Error! Bookmark not defined.
<u>2. Unit ID Display (applies to display units only)</u>	Error! Bookmark not defined.
<u>3. Announcement Call</u>	Error! Bookmark not defined.
<u>4. Repeater Talk Around (must be performed away from P1 Lab to avoid interference)</u>	Error!
Bookmark not defined.	
<u>5. Group Scan</u>	Error! Bookmark not defined.
<u>6. Transmit Lockout</u>	Error! Bookmark not defined.
<u>7. Late Entry</u>	Error! Bookmark not defined.
<u>8. VDOC Site Emergency Call Processing</u>	Error! Bookmark not defined.
<u>Appendix B – Aeronautical Permitted Radio Tests</u>	Error! Bookmark not defined.

Section

1

Permitted Radio Policy

1.1 Permitted Radio Policy

Prior to being permitted to operate on AFRRCS, all handheld and mobile radio models must successfully pass AFRRCS Permitted Radio testing and be included on the Permitted Radio List.

1.2 Effective Date

Permitted Radio Policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

Section

2

Appendix A – Permitted Radio Tests

1. Emergency ID and Alarm

Setup

Set Portable Radios 1, & 2 to Group 2, logged into system, on a multi channel site.

Execution

1. On Radio 1 press and hold the emergency button to declare an emergency. (A minimum time that the emergency button must be pressed may be configured into the Radio before an emergency is declared.)
2. Verify that the Emergency ID and Alarm shows up on Radio 2
3. Clear Emergency Alarm to proceed

2. Unit ID Display (applies to display units only)

Setup

Set Radio 1 and 2 to Talk Group 2, Logged into Site 1

Execution

1. PTT Radio 1 and hold. Verify that Radio 2 receives the call and displays the LID of Radio 1
2. Verify that the Radio Displays Unit ID.

3. Announcement Call

Setup

Radio 2 to Talk Group 2 and Radio 3 to Talk Group 3.

Execution

1. Place the All Call from console or supervisory radio
2. Audio should be heard at Radios 2 and 3.
3. Set Radio 2 to Talk Group 3.
4. Place the All Call from console or supervisory radio
5. Audio should be heard at Radios 2 and 3.

4. Repeater Talk Around (must be performed away from P1 Lab to avoid interference)

Execution

1. Place both radios on CH1 and PTT Radio 1 - verify audio is heard on radio
2. PTT Radio 2 – verify audio is heard on radio 1. Verify Repeater Talk Around feature.

5. Group Scan

Setup

Two radios (radio 1, radio 2) each with valid IDs and two valid groups (group 2, group 3) on selected system.

Radio 1 set up with group A and group B in the scan list, group A selected, and group scan initially disabled.

Execution

1. Place a call from radio 2 on talk group 2.
2. Verify the call is received and audio is heard on radio 1.
3. Place a call from radio 2 on talk group 3.
4. Verify the call is not received by radio 1.
5. Enable group scan on radio 1.
6. Place another call from radio 2 on talk group 3
7. Verify that the call is now received and audio is heard on radio 1.

6. Transmit Lockout

Setup – use single channel site for this test

Two radios (radio 1, radio 2) each with valid IDs and same valid group on selected system.

Talk group used for test must be set up as transmission trunked. This feature does not apply to message trunked calls.

Execution

1. Place a call from radio 1 on selected talk group by pressing and holding the PTT button.
2. Verify the call is received and audio is heard on radio 2.
3. While the call is in progress, press the PTT button on radio 2.
4. Verify that radio 2 does not transmit over (step on) the call in progress.

7. Late Entry

Setup

2 subscriber units, both turned off

Execution

1. Turn on Radio 1 (Group 2, logged into site 1) and PTT and talk.
2. While talking on Radio 1, Turn on Radio 2 (Group 2 logged into site 1).
3. Audio should be heard on Radio 2.

8. VDOC Site Emergency Call Processing

Objective

The purpose of this test is to verify that the subscriber unit registered to a VDOC (composite channel) Site can process emergency calls, when the control channel is temporarily unavailable and later becomes available.

Setup

The two radios used for this test must be capable of emergency calls.. The radios must be valid on the VDOC Site being used to conduct the tests.

Log Radio 1 and Radio 2 onto the VDoc used for this test. Ensure the radios are communicating on this system, when in the same Talk Group.

Execution

1. Verify the system initially logged into by Radios 1 & Radio 2 is Site the VDOC site. PTT Radio 1 and talk. The transmit (TX) indicators should turn on at Radio 1. Audio should be heard in Radio 2. The ID of Radio 1 should be seen at Radio 2.
2. Unkey Radio 1.
3. Press and hold the PTT on Radio 2. Immediately after pressing the PTT on radio 2, activate the Emergency Button on Radio 1 and hold down for 10 seconds. Release the Emergency Button on Radio 1, release the PTT on Radio 2 60 seconds after releasing the Emergency Button on Radio .
4. Verify that Radio 1 indicates the “TX EMER” declaration and that it reverts to the home group.
5. Verify that Radio 2 on VDOC Site (Site 2) indicate a “RX EMER” and hear audio on the emergency home group. Clear the emergency from Radio 1. Verify the emergency clears in the Radio 2.
6. Using the Radio 1, select the pre-stored ID of Radio 2 or enter the Radio 2 ID directly from the keypad, and PTT Radio 1. Verify that Radio 2 receives the call and displays the ID of Radio 1.
7. Release the PTT on Radio 1 and immediately PTT on Radio 2. Verify that Radio 1 receives the call and displays the ID of Radio 2.

Criteria for Success

Criteria for success is the subscriber unit successfully buffering the emergency call until a control channel is available to complete the call.

Section

3

Appendix B – Aeronautical Permitted Radio Tests

An established program exists for the testing and permitting subscriber radios onto the AFRRCS Radio network. Agencies with helicopters or airplanes require radios certified for airworthiness by Transport Canada, in addition to being permitted onto AFRRCS. The following requirements define the requirements for airborne AFRRCS radios.

Aeronautical Radio Requirements

An airborne FM radio is defined as a radio that is designed to be installed and operated in an aircraft. Primary power is from a 28 volt (nominal) negative ground aircraft power source.

- Airborne FM radios must be airworthiness approved by Transport Canada Civil Aviation (TCCA) or the FAA. A copy of the TCCA Authorized Release Certificate, Form One or equivalent must be included with each radio submitted for Permitted Radio testing.

The following tests must be successfully demonstrated by aeronautical radios.

1. **UNIT ID DISPLAY (APPLIES TO DISPLAY UNITS ONLY)**

Setup

Set Radio 1 and 2 to Talk Group 2, Logged into Site 1

Execution

1. PTT Radio 1 and hold. Verify that Radio 2 receives the call and displays the LID of Radio 1
2. Verify that the Radio Displays Unit ID.

2. **Simplex**

Setup

Radio 1 and Radio 2 must be programmed with Simplex frequency on Channel 1

Execution

1. Place both radios on CH1 and PTT Radio 1 - verify audio is heard on radio
2. PTT Radio 2 – verify audio is heard on radio

3. **GROUP SCAN**

Setup

Two radios (radio 1, radio 2) each with valid IDs and two valid groups (group 2, group 3) on selected system.

Radio 1 set up with group A and group B in the scan list, group A selected, and group scan initially disabled.

Execution

1. Place a call from radio 2 on talk group 2.
2. Verify the call is received and audio is heard on radio 1.
3. Place a call from radio 2 on talk group 3.
4. Verify the call is not received by radio 1.
5. Enable group scan on radio 1.
6. Place another call from radio 2 on talk group 3
7. Verify that the call is now received and audio is heard on radio 1.

4. LATE ENTRY

Setup

2 subscriber units, both turned off

Execution

1. Turn on Radio 1 (Group 2, logged into site 1) and PTT and talk.
2. While talking on Radio 1, turn on Radio 2 (Group 2 logged into site 1).
3. Audio should be heard on Radio 2.

5. TRANSMIT LOCKOUT

Setup – use single channel site for this test

Two radios (radio 1, radio 2) each with valid IDs and same valid group on selected system.

Talk group used for test must be set up as transmission trunked. This feature does not apply to message trunked calls.

Execution

1. Place a call from radio 1 on selected talk group by pressing and holding the PTT button.
2. Verify the call is received and audio is heard on radio 2.
3. While the call is in progress, press the PTT button on radio 2.
4. Verify that radio 2 does not transmit over (step on) the call in progress.

AFRRCS Policies and Procedures for Interoperability

Section: Programming Key Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	January 26, 2015	BS	First draft programming key policy
0.2	March 4, 2015	BS	As presented at I&S Council
0.3	March 9, 2015	KC	Formatted for signatures
1.0	March 22, 2016		Approved by Governance

Contents

<u>Programming Key Policy</u>	23
<u>1.1 Policy</u>	23
<u>1.2 Effective Date</u>	23

Section

1

Programming Key Policy

Programming of radios on the Permitted Radio list can be controlled for each agency limiting them to the talk groups they can access and radio IDs for that agency. There is no restriction placed on programming conventional mutual aid channels or the use of simplex.

The controls are enabled through the use of Master and Daughter programming keys. The manufacturers have all agreed to provide a Master programming key to AFRRCS for each of their permitted models. AFRRCS would provide a Daughter key configured correctly for the agency when it came onto the system. Daughter keys would require refresh every two years.

1.1 Policy

- a. AFRRCS will hold the master key which is able to create Daughter keys;
- b. Agencies will purchase a Daughter key when ordering radios, the Daughter key is to be delivered to AFRRCS;
- c. AFRRCS will program the provided Daughter key to match agency assigned resources. The keys will be set to expire within 2 years at which time the keys will need to be refreshed;
- d. The radio manufacturer must not distribute Master or Daughter keys directly to an agency;
- e. Payment for Daughter keys is the responsibility of the agency;
- f. Agency must notify AFRRCS if a Daughter key is lost or misplaced;
- g. AFRRCS will deny network access to any unauthorized radio(s).

1.2 Effective Date

Programming Key Policy shall become effective upon signature and shall remain in effect until rescinded. This policy shall be reviewed periodically and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Talkgroups

Contents

<u>Talkgroup Policies</u>	27
<u>1.1 Local Talkgroups</u>	27
<u>1.2 Shared Talkgroups (Interagency)</u>	27
<u>1.3 Common Event Talkgroup (CET)</u>	28
<u>Appendix</u>	29
<u>2.1 Talkgroup Example – Small Agency First Responder in Rural Alberta</u>	29

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	July 16, 2013	KC	Talkgroup guidelines approved by IS Council
0.2	August 13, 2013	KC	Draft Copy of Interoperability Guidelines with Encryption topic added. Introduction (including Council members), Purpose, and Roles and Responsibilities have been removed to a separate document.
0.3	October 11, 2013	KC	Updated the number of Talkgroups for each CET type to be smaller and more manageable.
0.4	January 23, 2014	KC	Updated based on feedback from Governance including removing requirement for each individual Talkgroup to have an SOP.
0.5	March 13, 2014	KC	Updated based on feedback from Alfred Klein to change appendix Talkgroup example to be a generic small first responder agency instead of a fire agency.
0.6	May 26, 2014	KC	Ready for submission to Governance reflecting latest changes from all groups in bold.
1.0	June 10, 2014		Approved by AFRRCS Governance.
1.1	November 6, 2015	KC	Annual policy review.
1.2	February 18, 2012	BS	Changed total of Provincial CET's to 16 from 5. Added emergency button policy for CETs is to be determined. Renamed Combined Event Talkgroups to Common Event Talkgroups.
2.0	March 22, 2016		Approved by AFRRCS Governance
2.1	October 21, 2016	KC	Added emergency button policies for CETs.
1.4	February 1, 2017	A Klein	Proposed draft to include Simplex CET programming
3.0	September 26, 2017	A Klein	Approved by AFRRCS Governance

Section

1

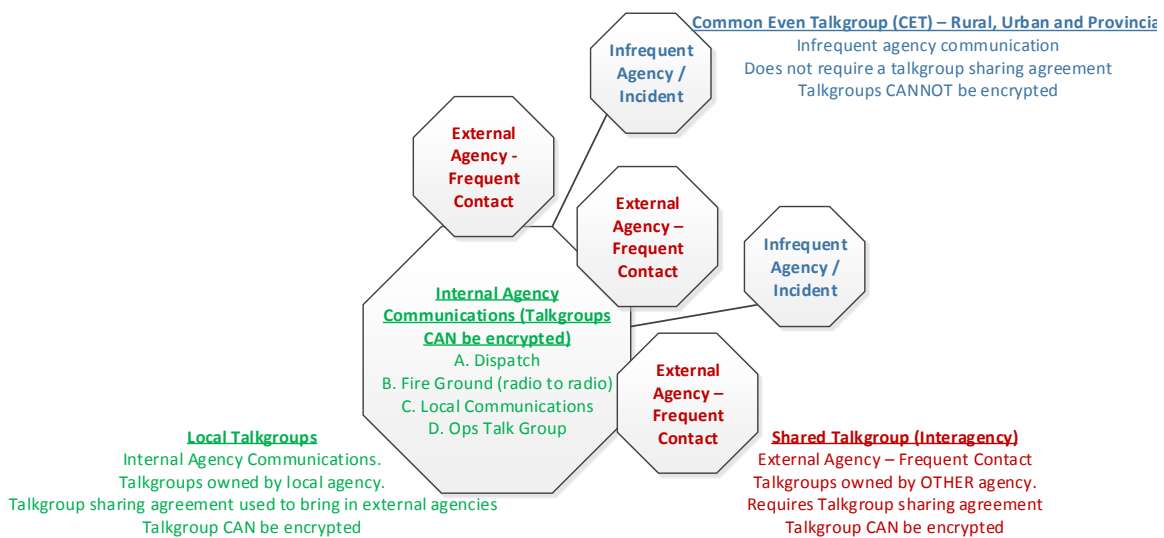
Talkgroup Policies

User Agency talkgroups are initially developed when the User Agency goes through the AFRRCS Transformation process with JSG. The transformation process provides guidance on setting up talkgroup structures as well as best practices. In the transformation process, the talkgroup plan is defined, and Operations, Maintenance and Sustainability (OMS) adds the talkgroup range into the AFRRCS UAS.

Note that each User Agency is responsible for programming their talkgroups into the AFRRCS UAS.

The following diagram illustrates a general talkgroup structure.

Diagram 1 AFRRCS Talkgroup Structure



1.1 Local Talkgroups

A local talkgroup is used when an agency is conducting internal communications.

Local Talkgroups Policy:

- a. An agency SOP should exist for the use of each local talkgroup.

1.2 Shared Talkgroups (Interagency)

A shared talkgroup is used when user agencies need to communicate with other user agencies on a frequent (recommended minimum weekly) basis.

Shared Talkgroup Policy:

- a. User agencies are responsible for their talkgroups and must give authorization for their talkgroups to be shared with another User Agency.
- b. An agency SOP shall exist for the use of shared talkgroups.
- c. Encryption shall be allowed on shared talkgroups. Encryption policies and procedures are the responsibility of the User Agency to define.
- d. Recording shall be allowed on shared talkgroups. Recording policies and procedures are the responsibility of the local User Agency to define.

1.3 Common Event Talkgroup (CET)

User Agencies that need to communicate with other User Agencies not frequently contacted, during special events or emergencies for example, can use Common Event Talkgroups (CET). There are three types of CETs (rural, urban, and provincial) that can enable communication on scene within a region or within the entire province.

Common Event Talkgroup Policy (CET):

- a. Agency Protocol (e.g. SOP, dispatch, local use, command) will direct users to the appropriate CET.
- b. Recording of CETs (TBD)
- c. The use of plain language is encouraged.
- d. Limit the use of acronyms or abbreviations as they can mean different things to different people.
- e. 1 CET shall exist in each of the defined Rural Operational Areas.
- f. 5 CETs shall exist for each of the seven defined urban districts.
- g. 16 CET provincial unassigned talkgroups shall exist. The provincial CET will be activated when the event occurs using AFRRCS operating procedures.
- h. CETs should be used for on scene command coordination only.
- i. CETs are unrestricted and open to all AFRRCS agencies. Requests from first responder agencies to activate a Provincial CET should not be denied.
- j. Dispatch verifies if the talkgroup is clear for urban CETs. Incidents take priority.
- k. All AFRRCS radios shall be programmed for the CETs used in the agency response area and the 16 provincial CETs.
- l. OMS will notify all public-safety answering points (PSAP) on AFRRCS, using a distribution list, when province Common Event Talkgroups are activated and when they are deactivated.
- m. All radios will be programmed so that Emergency button declarations on provincial CETs shall stay on that talkgroup.

1.4 Simplex AFRRCS

User Agencies that need to communicate with other User Agencies not frequently contacted, during special events or emergencies for example, can use simplex, direct line of sight communications. There are five AFRRCS licensed simplex frequencies included in the AFRRCS CETs.

Due to the intended interoperable nature of AFRRCS simplex frequencies, these channels are not to be programmed with encryption. It is recommended for agencies that have encrypted simplex requirements to directly liaise with Innovation, Science and Economic Development Canada. (ISED)

- a. Simplex CETs should be programmed as a P25 conventional frequency in a digital format with the default TX NAC: \$293 (HEX) or 659 (decimal) (US Department of Homeland Security National Interoperability Field Operations Guide (NIFOG)).
<https://www.dhs.gov/sites/default/files/publications/National%20Interoperability%20Field%20Operations%20Guide%20v1%206%201.pdf>
- b. Use of the simplex frequencies may be guided by local AFRRCS agencies as required
- c. Simplex frequencies are frequently used for Incident Scene Command for multi-agency events. AFRRCS user agencies should consider using AFRRCS SIMP1 (770.18125 MHz) as the default incident scene channel and that the users have convenient access to the channel programmed in their radios.

Section

2

Appendix

2.1 Talkgroup Example – Small Agency First Responder in Rural Alberta

Communication Requirements:

- Local communication are required between
 - Dispatch and Responders
 - Responders Radio to Radio
 - Local Communications
 - Operations
- Communications with neighbouring MDs
 - Municipal District “A” (more than weekly)
 - Municipal District “B” (yearly)
- Communications on ad-hoc emergency basis or other events in surrounding areas
 - Estimate max 3 simultaneous events possible



AFRRCS Policies and Procedures for Interoperability

Section: Coverage Class Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	October 23, 2014	BS	First draft version Coverage Class Policy
0.2	December 3, 2014	KC	First version approved by IS Council
1.0	December 17, 2014		Approved by AFRRCS Governance
1.1	November 6, 2015	KC	Annual policy review
1.2	November 19, 2015	BS	Reviewed annual policy review with IS Council
2.0	June 21, 2016		Annual policy review approved by Governance

Contents

Coverage Class Policy 33

1.1 Coverage Class Policy 33

1.2 Effective Date 33

Section

1

Coverage Class Policy

The coverage provided to each talkgroup is through the selection of a Coverage Class. Coverage Classes are defined by the System Administrator, for assignment by the Agency Administrator to their talkgroups. A Coverage Class is the definition of what geography the talkgroup is operative within.

1.1 Coverage Class Policy

- a) Agency talkgroups are to provide coverage within the operational area for that agency.
- b) Geographically Defined Common Event Talkgroups (CET) are to provide coverage within that **jurisdiction** and each **jurisdiction** adjacent to the primary **jurisdiction**.
- c) Common Event Talkgroups (CET) assigned to the seven urban areas are to provide coverage within the boundaries of that city + a radius of 50 kilometres around the city limits.
- d) Province Wide Common Event Talkgroups (CET) are assigned a Coverage Class based on the request of the Incident Commander.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Talkgroup Naming Conventions

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	January 23, 2015	BS	First draft Talkgroup Naming Conventions
0.2	March 4, 2015	BS	As amended at March 4 IS Council meeting
0.3	March 9, 2015	KC	Formatted for final approval
1.0	June 23, 2015		Approved by AFRRCS Governance Council
1.1	April 6, 2016	KC	Formatted for annual review
1.2	June 2, 2016	KC	Annual review by IS Council
2.0	June 21, 2016		Annual review approved by Governance
2.1	October 21, 2016	KC	Removed appendix A naming conventions to use the AFRRCS design document as the source of truth. Amended wording associated with Appendix A.

Table of Contents

<u>Talkgroup Naming Conventions</u>	37
<u>1.1 Talkgroup Naming Conventions</u>	37
<u>1.2 Effective Date</u>	37

Section

1

Talkgroup Naming Conventions

There are three categories of talkgroups within AFRRCS:

1. Agency specific talkgroups, which are for the day to day use of the specific agency.
2. Geographically defined Common Event Talkgroups (CET's), assigned on a fixed basis to each rural municipality and the seven urban areas.
3. Province wide Common Event Talkgroups (CET's), assigned with a specific coverage, as required.

1.3 Talkgroup Naming Conventions

- a) Talkgroups assigned for the use of specific agencies are to be named according to the standards established by the agency assigned the talkgroup.
- b) Geographically assigned CETs (one per county, five for each of the seven urban areas) will follow the three digit numbering scheme for that jurisdiction, as listed in the attached Municipal Affairs 2015 Municipal Codes. Special Areas will be assigned one CET, with the designation number 464. Those areas assigned more than one CET will append a dash plus 1 digit identification for each of their assigned CET's i.e. City of Calgary 046-1, 046-2. Assigned Common Event Talkgroup (CET) designation not to be aliased in user radio.
- c) Province Wide CET's will be assigned the designations AFRRCS01 to AFRRCS16. Assigned Common Event Talkgroup (CET) designation not to be aliased in user radio.

1.4 Effective Date

Talkgroup Naming Conventions Policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Talkgroup Priority

Contents

Contents

<u>Talkgroup Priority Policy</u>	41
<u>1.1 Talkgroup Priority Policy</u>	41
<u>1.2 Effective Date</u>	41

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	October 23, 2014	BS	First draft version Talkgroup Priority Policy
0.2	March 4, 2015	BS	Final version approved by Interoperability & Standards Council
1.0	June 23, 2015		Approved by AFRRCS Governance Council
1.1	April 6, 2016	KC	Formatted for annual review
1.2	June 2, 2016	KC	Annual review by IS Council
2.0	June 21, 2016		Annual review approved by Governance

Section

1

Talkgroup Priority Policy

Trunked radio systems provide the opportunity to prioritize some talkgroups at a higher level than other talkgroups. This only comes into play if calls are queued, waiting for resources, at a repeater site. Higher priority talkgroups are placed higher in the queue for those resources than lower priority talkgroups. Higher priority calls do not pre-empt calls that are in process

1.1 Talkgroup Priority Policy

- a) Common Event Talkgroups (CETs) will not be assigned a higher or lower priority than first responder agency talkgroups.
- b) First responder agency talkgroups will have a higher priority level than secondary responder talkgroups.
- c) Individual agencies may choose to assign different priorities within their own talkgroups i.e. Training TG lower priority than Event TG.

1.2 Effective Date

Talkgroup Priority Policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Patching Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	January 27, 2016, 2014	BS	First draft version of the Patching Policy
0.2	February 18, 2016	BS	Approved by IS Council
0.3	February 22, 2016	KC	Formatted for Governance review
0.4	March 14, 2016	BS	Added the use of consoles that support System Assigned IDs to be exempt from the limitation of patching 2 talkgroups.
1.0	March 22, 2016		Approved by AFRRCS Governance

Contents

<u>Patching Policy</u>	45
<u>1.1 Patching Policy</u>	45
<u>1.2 Effective Date</u>	45

Section

1

Patching Policy

Approximately 80% of AFRRCS sites have four channels, one channel is dedicated for controlling leaving three available channels for voice traffic. An issue was found when patching talkgroups with non-Harris consoles that a channel is required for each patch, this could easily tie up most AFRRCS sites. Patching three talkgroups together consumes the total number of channels. Patching four or more talkgroups produces an unpredictable result.

1.1 Patching Policy

Patching policies:

- e) For multiagency communications, users should be directed to a shared talkgroup or Common Event Talkgroup when possible;
- f) All agencies should design their talkgroups to minimize the use of patching
- g) Dispatchers should not patch more than two AFRRCS talkgroups together. If the combination of more AFRRCS talkgroups is required, intra-agency communications, users should be directed to an agency tactical talkgroup or Common Event Talkgroup
- h) Consoles utilizing a System Assigned ID (SAID) to create a new combined talkgroup at the system level will be deemed exempt from (c) of this patching policy.
- i) OMS reserves the right to limit the use of patching to preserve system integrity

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Unconfirmed Talkgroup Policy

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	January 27, 2016, 2014	BS	First draft version of the Unconfirmed Talkgroup Policy
0.2	February 18, 2016	BS	Approved by IS Council
0.3	February 22, 2016	KC	Formatted for Governance review
1.0	March 22, 2016		Approved by AFRRCS Governance

Contents

<u>Unconfirmed Talkgroup Policy</u>	49
<u>1.1 Unconfirmed Talkgroup Policy</u>	49
<u>1.2 Effective Date</u>	49

Section

1

Unconfirmed Talkgroup Policy

Confirmed Talkgroups do not permit a call to be established until radio channel resources are available to support all of the users in the talkgroup. This feature gives users confidence that all of their colleagues are participating in a call, but when the system is under high load it can result in call delays.

Unconfirmed Talkgroups are permitted to start even if the system can only support a subset from the outset. As radio channel resources free up, additional users are able to join the call. This mode of operations allows the call to begin quickly, particularly in times of high usage.

1.1 Unconfirmed Talkgroup Policy

- a. AFRRCS Talkgroups are to be configured as unconfirmed talkgroups.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Agency Interoperability Contact

Contents

Agency Interoperability Contact Policies and Procedures 53

1.1 Agency Interoperability Contact Policy..... 53

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	June 2, 2016	KC	Created from IS Council policy recommendation
1.0	June 21, 2016		Approved at Governance

Section

1

Agency Interoperability Contact Policies and Procedures

In order to provide the highest level of Interoperability and mutual aid services to the residents of Alberta, responding agencies must have access to interoperable communications. It is the intent of this policy to provide a means for agencies to contact other agencies for information on setting up shared talkgroups.

1.1 Agency Interoperability Contact Policy

Each agency shall name an interoperability contact which will be the Agency Administrator or designee. AFRRCS will collect names of agency interoperability contacts and make available to other agencies upon request.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: PTT Voice Primary Service

Contents

PTT Voice Primary Service 57

1.1 Policy..... 57

1.2 Effective Date..... 57

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	November 19, 2015	BS	First draft
0.2	November 19, 2015	BS	Reviewed with IS Council
1.0	June 21, 2016		Approved by Governance

Section

1

PTT Voice Primary Service

AFRRCS was designed and implemented to support PTT voice traffic between users. Additional network applications involving data may interfere with the efficient transmission of PTT voice traffic.

1.1 Policy

Carriage of PTT voice traffic is the primary purpose for AFRRCS. Any additional application that interferes with the voice traffic must be controlled or prohibited. New applications must be evaluated prior to use.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Data Primary Service

Contents

<u>Data Primary Service</u>	57
<u>1.1 Policy</u>	57
<u>1.2 Effective Date</u>	57

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	February 1, 2017	A Klein	DRAFT
1.0	September 26 2017	A Klein	Approved by AFRRCS Governance

Section

1

Data Primary Service

AFRRCS was designed and implemented to support small data applications. AFRRCS is not intended to replace an agencies primary data handling services. Inefficient network applications may interfere with the transmission of PTT voice and other data traffic.

1.1 Policy

Carriage of PTT voice is a primary purpose for AFRRCS.

Efficient data applications may replace or reduce an agencies PTT voice requirements thereby ensuring site availability for all users.

Agency data applications should replace PTT voice calls and be should be oriented to First Responder and Public Safety.

Agency transmission of data messages to the AFRRCS system should be by means of a direct connection as CAI interfaces may degrade local PTT voice capacity.

Examples of data messages include:

- Emergency Event Alerting (Paging)
- Location services related to EAB activation
- Location service related to on-event personal level tracking
- Status messaging
- OTAR (will not replace PTT voice for any agency as voice has pre-emption priority over OTAR)
- Request to Talk (RTT)
- Emergency Request to Talk (ERTT)

New applications may interfere with voice traffic and must be evaluated by I&S and AFRRCS OMS.

New applications may require the development of new policies to guide their development and use.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Trunking Features

Contents

<u>Trunking Features Policies and Procedures</u>	65
<u>1.1 Simulselect</u>	65
<u>1.2 Announcement Call</u>	65
<u>1.3 Dynamic Regrouping</u>	65
<u>1.4 Individual Call (I-Call)</u>	66
<u>1.5 GPS Usage</u>	66
<u>1.6 Texting</u>	66
<u>1.7 Effective Date</u>	66

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	March 16, 2014	KM	First Draft
0.2	May 15, 2015	BS	Confirmed content with fleetmapping workgroup
0.3	October 20, 2015	KC	Removed Vita Telephone Interconnect (VTI), GPS, and texting to be deferred for future consideration.
0.4	November 10, 2015	KC	Added VTI, GPS, and texting functionality.
0.5	November 19, 2015	BS	Reviewed with the IS Council, removed VTI.
1.0	June 21, 2016		Approved by Governance

Section

1

Trunking Features Policies and Procedures

This document describes the trunking features available on AFRRCS and the associated policies and procedures. For more specific information on features consult with the AFRRCS OMS.

1.1 Simulselect

Simultaneous Select allows a console operator to communicate with two or more talkgroups by assigning the groups to a common System Assigned ID (SAID) Simulselect is primarily used for console initiated broadcasts to all channels/groups within select areas of an organization.

Policy:

- a. It is highly recommended that the personnel activating the Simulselect be trained in the operational techniques necessary for proper communication and system efficiency.

1.2 Announcement Call

An announcement group is a higher level group which is composed of a number of talkgroups. It permits a dispatcher to make one broadcast style call to all talk groups that have the Announcement talkgroup assigned to it. This can allow communication to an entire agency, fleet or across multiple agencies. Each talk group has an optional announcement group, which is provisioned to the radio by the channel during registration.

Policy:

- a. It is highly recommended that the personnel activating the Announcement Call be trained in the operational techniques necessary for proper communication and system efficiency. All users should be trained on their agency's proper use of announcement calls.

1.3 Dynamic Regrouping

The dynamic regrouping feature allows an authorized system administrator (with appropriate access), via the UAS, to assign a radio to a specific talkgroup remotely. The purpose of this feature is to allow multiple radios to be grouped together on a talkgroup for operational purposes. This feature is limited in function due to the potential delays while the radio is assigned to the new talkgroup; because of this, few agencies use this for critical operations

This feature also must be enabled in the subscriber units and is not supported by all permitted radios.

This feature is **not** supported by AFRRCS.

1.4 Individual Call (I-Call)

A private call is placed from one field radio to another or from a dispatcher to a field radio by using that callee's unique ID number.

Policy:

- a. It is highly recommended that the personnel implementing the I-Call be trained in the operational techniques necessary for proper communications.
- b. I-call can be enabled on the network for utilization by those agencies who desire it
- c. Each agency have the responsibility to determine whether they wish to implement I-Call for their users.
- d. Each agency is responsible for the administration and management of their own I-Call implementation.
- e. The timer for I-Calls be set to 30 seconds.
- f. Single channel sites will be initially configured **not** to support I-calls.

1.5 GPS Usage

P25 can support applications that generate <9.6kbit/s data flows. GPS is an application used by first responders, but if not configured correctly it could seriously hamper the responsiveness and availability AFRRCS voice services.

Policy:

- a. Agencies can implement testing of GPS services over AFRRCS, if approved by the OMS.
- b. An application to the OMS for use GPS services on AFRRCS must include the number of proposed users, polling rates, what triggers polling, coverage area.
- c. If AFRRCS determines that the use of GPS data is or could negatively impact AFRRCS GOS, AFRRCS reserves the right to restrict or modify agency use of GPS.
- d. When available, OMS will publish a model for acceptable GPS usage.
- e. Workgroup to develop suggested best practices for GPS implementation.

1.6 Texting

Texting would support communication from radio to radio, and radio to computer aided dispatch (CAD) or vice versa. Its use will be monitored and is assumed to not compromise delivery of essential services.

Policy:

- a. Agencies can implement testing of texting over AFRRCS, if approved by the OMS.
- b. An application to the OMS for using texting on AFRRCS must include the number of proposed users and texting traffic.
- c. If AFRRCS determines that the use of texting is or could negatively impact AFRRCS GOS, AFRRCS reserves the right to restrict or modify agency use of texting.

1.7 Effective Date

Trunking Features policy shall become effective upon signature and shall remain in effect until rescinded. This policy shall be reviewed periodically and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: AES, and KMF Vendor

Contents

<u>AES and KMF Vendor Policies</u>	70
<u>1.1 Encryption Policy</u>	70
<u>1.2 Effective Date</u>	70

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	March 17, 2014	KC	Encryption policy and procedure for Encryption Work Group second reading.
0.2	March 27, 2014	BS	Amendments made by Encryption Workgroup
0.3	May 22, 2014	KC	Version 1
1.0	December 17, 2014		Approved by AFRRCS Governance
1.1	November 7, 2015	KC	Annual policy review
1.2	November 19, 2015	BS	Annual policy review with IS Council
2.0	June 21, 2016		Annual policy review approved by Governance

Section

1

AES and KMF Vendor Policies

AFRRCS, as well as some subscriber radios, support both AES 256 bit encryption and DES encryption. AES, a newer more robust encryption algorithm that has generally replaced DES, has been set as the encryption standard for AFRRCS. Standardizing on one algorithm will simplify interagency communications where encryption is required and provide a more secure environment for users.

No KMF manufacturers who made presentations to the AFRRCS Encryption Workgroup, except Harris, had a product that would successfully and directly connect to a Harris P25 VIDA network.

A Harris, or non- Harris “manual key-loading device” could be used if desired by agencies. All manual key-loading devices should be tested prior to implementation on AFRRCS.

1.1 Encryption Policy

AES shall be the only encryption algorithm used by AFRRCS agencies, unless otherwise approved by OMS.

Agencies utilizing encryption on AFRRCS and who desire the use of a network-connected Key Management Facility (KMF) shall use a Harris KMF.

1.2 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: Link Layer Authentication

Contents

<u>Link Layer Authentication Policies and Procedures</u>	74
<u>1.1 Link Layer Authentication Policy</u>	33
<u>1.2 Effective Date</u>	9

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
1.0	May 22, 2014	Kris Cottrell, PMP, CBAP	First version of Link Layer Authentication policies and procedures.
1.0	June 10,2014		Approved at Governance

Section

1

Link Layer Authentication Policies and Procedures

Link layer authentication is a method by which the radio network can “challenge” subscriber units attempting to acquire network service. When a radio requests service from a tower, the network checks the UAS database to determine whether that radio must be authenticated by LLA. If the database shows that radios from that agency require LLA, the subscriber unit must present a network “key”.

LLA can be enabled by agency, group of radios or individual radios.

The network is entered into the radio by a key loading device. The key is loaded once for each radio being added to the network.

Each agency determines for itself whether it wishes to utilize LLA.

The subscriber unit can also be programmed to demand proof from the network that it is the desired P25 network.

When LLA is implemented, radios cannot be “cloned” from existing users and gain access to the network. Information from lost or stolen radios cannot be copied to other radios, giving them access to the talkgroups programmed into the lost or stolen radio.

1.1 Link Layer Authentication Policy

- a) LLA be enabled on the network for utilization by those agencies who desire it
- b) Each agency have the responsibility to determine whether they wish to implement LLA for their users
- c) Each agency responsible for the administration and management of their own LLA implementation.

1.2 Effective Date

Agency Component Testing policy shall become effective upon signature and shall remain in effect until rescinded. This policy shall be reviewed periodically and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: OTAR

Contents

<u>OTAR Policies and Procedures</u>	78
<u>1.1 OTAR Policy</u>	78
<u>1.2 OTAR Procedures</u>	78
<u>1.3 Effective Date</u>	78

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	March 17, 2014	KC	For second reading by Encryption WG
0.2	March 27, 2014	BS	Amendments made by Encryption Workgroup
0.3	May 27, 2014	KC	Version 1.
1.0	December 17, 2014		Approved by AFRRCS Governance.
1.1	November 6, 2015	KC	Annual policy review
1.2	November 19, 2015	BS	Annual policy review with IS Council
2.0	June 21, 2016		Annual policy review approved by Governance

Section

1

OTAR Policies and Procedures

Over-the-Air-Rekeying (OTAR) is the process for changing a Traffic Encryption Key (TEK) or Key Encryption Key (KEK) in a radio or device by sending a new key directly to the radio or device over the communication path it secures.

1.1 OTAR Policy

OTAR shall not be undertaken during network busy periods. Scheduling is to be negotiated with Operations Management Sustainability (OMS).

If a network event occurs that makes reprogramming inadvisable, OMS must notify agencies scheduled for reprogramming and arrange an alternative time.

Data usage for four channel sites shall be restricted to one channel, two channel at eight channel sites, three at twelve channel sites.

1.2 OTAR Procedures

A crypto-officer must be appointed for agencies using encryption. Minimum training requirements for Crypto-officer will be provided by the Interoperability & Standards Council.

Rekeying and programming frequency are determined on an agency basis, and scheduling must be approved by OMS.

Emergency re-keying of 100 or fewer radios is permitted as required. Emergency rekeying of more than 100 radios is to be approved by OMS. Emergency rekeying can be supported by OMS partitioning of the data channel, as required.

AFRRCS will provide troubleshooting procedures for OTAR, as it pertains to the network. Prior to an agency implementing OTAR the OMS must verify that there is no negative impact on the AFRRCS network. AFRRCS will provide facilities for this testing.

OMS reserves the right to limit the use of OTAR to preserve system integrity.

1.3 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS Policies and Procedures for Interoperability

Section: OTAP

Contents

<u>OTAP Policies and Procedures</u>	82
<u>1.1 OTAP Policy</u>	82
<u>1.2 OTAP Procedures</u>	82
<u>1.3 Effective Date</u>	82

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	March 17, 2014	KC	For second reading by Encryption WG
0.2	March 27, 2014	BS	Amendments made by Encryption Workgroup
0.3	May 27, 2014	KC	Version 1.
1.0	December 17, 2014		Approved by AFRRCS Governance
1.1	November 6, 2015	KC	Annual policy review
1.2	November 19, 2015	BS	Annual policy review with IS Council
2.0	June 21, 2016		Annual policy review approved by Governance

Section

1

OTAP Policies and Procedures

Over-the-Air Programming (OTAP) provides the capability to change the radio's entire personality and features over the air. Changes to a radio's specific personality, such as talkgroup affiliation, user preferences, access to system features, etc., are transmitted over the air to the radio. User agencies will have an easier, less time-consuming method of managing their radios.

1.1 OTAP Policy

OTAP or shall not be undertaken during network busy periods. Scheduling is to be negotiated with Operations Management Sustainability (OMS).

If a network event occurs that makes reprogramming inadvisable, the OMS must notify agencies scheduled for reprogramming and arrange an alternative time.

1.2 OTAP Procedures

Programming frequency is determined on an agency basis, and scheduling must be approved by the OMS.

Emergency programming of 100 or fewer radios is permitted as required. Emergency programming of more than 100 radios is to be approved by OMS. Emergency programming can be supported by OMS partitioning of the data channel, as required.

AFRRCS will provide troubleshooting procedures for OTAP as it pertains to the network. Prior to an agency implementing OTAP the OMS must verify that there is no negative impact on the AFRRCS network. AFRRCS will provide facilities for this testing.


OMS reserves the right to limit the use of OTAP to preserve system integrity.

1.3 Effective Date

This policy shall become effective upon approval and shall remain in effect until rescinded. This policy shall be reviewed yearly and updated when required.

AFRRCS

Agency Network Connectivity Policy

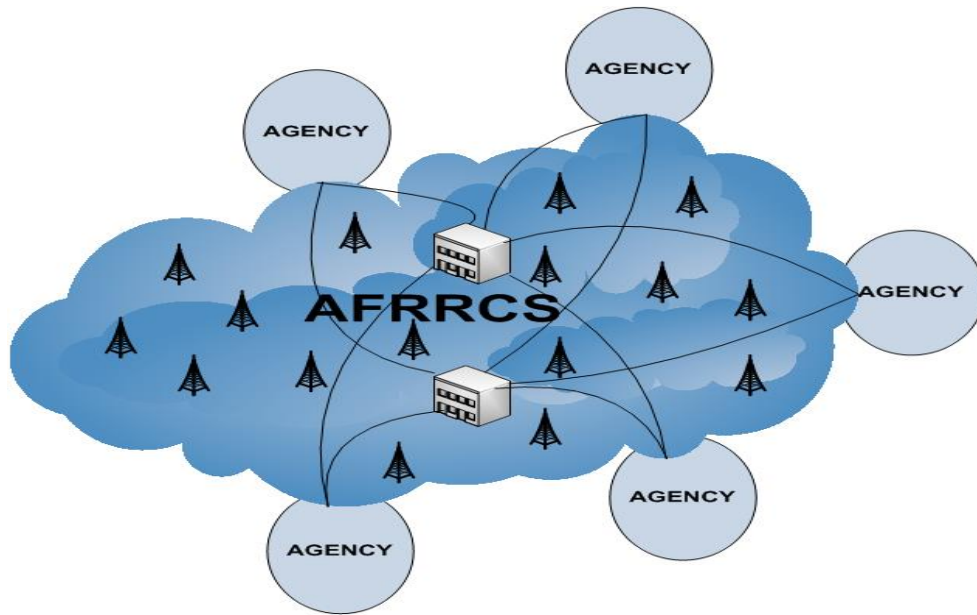


1	<u>Introduction</u>	86
2	<u>Connectivity Handbook</u>	87
4	<u>Definitions</u>	87

Version	Revision Date	Reviser	Details
0.1	2015	KM	First Version
0.2	June 18, 2015	AM	Second Revision
0.3	July 6, 2015	AM	Third Revision – Includes corrections provided
0.4	July 10, 2015	AM	Title Change
0.5	July 29, 2015	AM	Fourth Revision – Includes additional Edge device requirements
0.6	September 14, 2015	AM	Further clarification on demark point
0.7	October 6, 2015	KC	Minor Updates
1.0	January 26, 2017	JD	Updated and Revised
2.0	October 30, 2017	MQ	Revised to Policy and SOP
2.1	November 7, 2017	EP	Revised PSAP definition

Introduction

AFRRCS Agency Connectivity



AFRRCS has been designed to facilitate communications between first responder agencies throughout the province. To accomplish this goal, the AFFRCS network includes standard methods to provide agencies access for devices requiring direct connectivity to the Network Switching Centers and for systems used for agency radio administration.

AFRRCS can support both native Harris and non-native connection of PSAP devices.

User agencies will also require connection to AFRRCS to support user configuration of the UAS. This connection can only be done through the VPN connection.

Connectivity Handbook

AFRRCS OMS will maintain a handbook outlining the technical specifications and configuration requirements for agency connection to AFRRCS. The handbook is available from the AFRRCS OMS assigned BRM or the AFRRCS Transformation consultant.

Definitions

Agency-AFRRCS Edge Device: a network device which resides on the Agency premise and contains the configuration to support AFRRCS connectivity. In situations where the Agency requires or prefers redundancy in AFRRCS connectivity two or more edge devices will be required.

Agency Device: equipment, devices or interfaces that are located on the Agency premise and are incorporated into the AFRRCS system. Examples of Agency Devices include: consoles, voice loggers, Key Management Facility (KMF), and Computer Aided Dispatch (CAD).

Network Switching Center (NSC): The NSC's provide the centralized applications, services and converged communications for AFRRCS radio network. AFRRCS has redundant NSC's in Edmonton and Calgary to provide province wide fail over capabilities.

Public Safety Access Point (PSAP): Agency dispatch location.

Standard Operating Procedures (SOP) manual: AFRRCS publication documenting the current setup and configuration requirements for this policy.

AFRRCS Policies for Operations

Section: Provincial Emergency Support and
Deployed Operations

Contents

<u>Provincial Emergency Support and Deployed Operations Policy</u>	91
<u>1.1 Deployment Overview</u>	91
<u>1.2 Deployment Authorized Uses Policy</u>	91
<u>1.3 Deployment Policy</u>	91
<u>1.4 Effective Date</u>	92

DOCUMENT REVISION HISTORY

Version	Date	Modified By	Section, Page(s), Text Revised
0.1	March 17, 2014	KC	Site on Wheels (SoW) Deployment Request approved by IS Council
0.2	May 26, 2014	KC	Updated based on feedback from IS Council for SoW location for storage and organization that would manage and prioritize requests.
1.0	December 17, 2014		Approved by AFRRCS Governance Council
1.1	April 28, 2015	MQ	Updated previous SoW deployment policy including renaming the policy and adding procedures.
1.2	May 7, 2015	MQ	Update after review. All sections.
1.3	June 24, 2015	MQ	All sections with input from AEMA POC.
1.4	June 30, 2015	KC	Edited for final approvals.
1.5	May 2, 2016	MQ	Edited after annual review
1.6	October 23, 2016	MQ	Edited IAW Governance direction
1.7	October 24, 2016	KC	Edited for final approvals
1.8	November 23, 2017	GJB	Updated IMT inclusion

Section

1

Provincial Emergency Support and Deployed Operations Policy

1.1 Deployment Overview

This deployment policy covers four separate resources:

- Radio Cache 1, 100 handheld radios
- Radio Cache 2, 100 handheld radios
- Radio Cache 3, 100 handheld radios
- Radio Cache 4, 100 handheld radios
- Site on Wheels 1, mobile four repeater site
- Site on Wheels 2, mobile four repeater site

The Site on Wheels (SoW) is a fully featured 4 channel, 700 MHz P25 trunked site with satellite backhaul to the network core providing quick deployment of portable communications coverage virtually anywhere in Alberta.

1.2 Deployment Authorized Uses Policy

AFRRCS will deploy resources to support the following:

- a. In support of an emergency situation requiring augmentation of the communications available within a region or municipality;
- b. In support of AFRRCS site failures that require the replacement or augmentation of the site;
- c. In support of a municipal or agency event or operation that requires the augmentation of the present or existing communications capability;
- d. In support of an Incident Management Team (IMT) deployed to an emergency or disaster;
- e. In support of an AFRRCS engineering or operations exercise.

1.3 Deployment Policy

- a. The requesting organization will be responsible for covering the cost of the AFRRCS deployment;
- b. The requesting organization is responsible for ensuring that the radios are not lost or damaged through misuse or abuse. The organization will be responsible for replacement of lost or damaged radios not consistent with the normal operational use of the portable radios. The assessment of damage is at the sole discretion of AFRRCS;
- c. In the event that the requesting organization is not an AFRRCS user agency, having a signed user agreement with AFRRCS, the request for deployment must be approved by the ADM responsible for AFRRCS. The exception would be deployments on behalf of the Alberta Emergency Management Agency (AEMA), Provincial Operations Centre (POC) in response to an emergency or disaster requiring provincial coordination;
- d. IMTs who request AFRRCS communications support in relation to a coordinated AEMA response, can do so via a request to the AEMA POC. Once approved for funding and deployment, the POC will provide AFRRCS with a tasking number. Should the IMT request AFRRCS communications as part of a mutual aid request and not in support of an AEMA coordination, the IMT and municipality will be responsible to fund the AFRRCS deployment;

- e. AFFRCS will be responsible for determining which assets are deployed to meet the communications needs of the requesting entity;
- f. The requesting organization is responsible for suitable security measures (operation dependant); and;
- g. In special situations the requesting agency will be responsible to provide or coordinate accommodations, meals, and administrative support.

1.4 Effective Date

This policy shall become effective and shall remain in effect until rescinded. This policy shall be reviewed periodically and updated when required.