Alaska Land Mobile Radio Communications System

System Key Usage Procedure 400-16

Version 6

May 30, 2018

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	3/6/2013	New procedure; approved by the User Council - final.	1
Shafer, Sherry	3/6/2014	Annual review/update. Approved by the Operations Management Office - final.	2
Shafer, Sherry	3/23/2015	Annual review/update. Approved by the Operations Management Office - final.	3
Shafer, Sherry	3/18/2016	Annual review. Approved by the Operations Management Office - final.	4
Shafer, Sherry	3/3/2017	Annual review. Approved by the Operations Management Office - final.	5
Shafer, Sherry	5/30/2018	Annual review. Approved by the User Council - final.	6

Acronyms and Definitions

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that operate on the shared ALMR system infrastructure.

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, which uses but is separate from the State of Alaska Telecommunications System (SATS), as established in the Cooperative and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

Department of Defense – Alaska: Alaskan Command, US Air Force and US Army component services operating under United States Pacific Command and United States Northern Command.

Executive Council: the ALMR Executive Council which is made up of three voting members and two associate members representing the original four constituency groups: the State of Alaska, the Department of Defense, Federal Non-DOD agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage).

Federal Communications Commission (FCC): for the purposes of ALMR, the Federal level governing body that approves the use of commercial, maritime, state, local and other agencies that are not a part of the Department of Defense or other Federal agencies radio frequency spectrum through the issuance of radio station authorizations once coordination with all potentially affected agencies has been completed. The approvals will in most cases (exceptions might be waivers or special temporary authority) be for use of a particular portion of a frequency band that has been pre-authorized through the frequency band table of allocations. In addition, the FCC maintains the communications tower registration program.

Local Governments: those Alaska political subdivisions defined as municipalities in AS 29.71.800(13).

Member: a public safety agency including, but not limited to, a general government agency (local, state or federal), its authorized employees and personnel (paid or volunteer), and its service provider, participating in and using the System under a Membership Agreement.

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of over 300,000. The MOA stretches from Portage, at the southern border, to the Knik River at the northern border, and encompasses the communities of Girdwood, Indian, Anchorage, Eagle River, Chugiak/Birchwood, and the native village of Eklutna.

Operations Management Office (OMO): develops recommendations for policies, procedures, and guidelines; identifies technologies and standards; and coordinates intergovernmental resources to facilitate communications interoperability with emphasis on improving public safety and emergency response communications.

P25 Standards: the P25 suite of standards involves digital land mobile radio (LMR) services for local, state and national (federal) public safety organizations and agencies. P25 is applicable to LMR equipment authorized or licensed, in the U.S., under the National Telecommunications and Information Administration (NTIA) or Federal Communications Commission (FCC) rules and regulations.

State of Alaska (SOA): the primary maintainer of the SATS (the State's microwave system), and shared owner of the System.

State of Alaska Telecommunications Systems (SATS): the State of Alaska statewide telecommunications system microwave network.

System Management Office (SMO): the team of specialists responsible for management of maintenance and operations of the System.

User Council: the User Council is responsible for recommending all operational and maintenance decisions affecting the System. Under the direction and supervision of the Executive Council, the User Council has the responsibility for management oversight and operations of the System. The User Council oversees the development of System operations plans, procedures and policies under the direction and guidance of the Executive Council.

User: an agency, person, group, organization or other entity which has an existing written Membership Agreement to operate on ALMR with one of the Parties to the Cooperative and Mutual Aid Agreement. The terms user and member are synonymous and interchangeable.

1.0 Purpose

The Operations Management Office (OMO) and System Management Office (SMO) are committed to improving communications and providing information and technical assistance for the Alaska Land Mobile Radio (ALMR) Communications System ensuring maximum benefit for the stakeholders and the agencies that utilize it, while maintaining the integrity and security of the System at the highest levels.

Responsibilities outlined in this document apply to any individuals that utilize or support the ALMR System.

2.0 Roles and Responsibilities

2.1 Executive Council

The Executive Council (EC) shall be responsible for the management and enforcement of sanctions when violations of the System Key Usage Procedure warrant such action(s).

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the System Key Usage Procedure, and any substantial revisions hereafter.

2.3 Operations Management Office

The Operations Management Office (OMO) provides oversight of the day-to-day operations of the ALMR System on behalf of the User and Executive Councils.

The OMO will ensure an audit of System Keys is performed by the System Management Office every year.

2.4 System Management Office

The System Management Office (SMO), as the primary System Key holder, is responsible for managing all System Key technology.

The SMO will:

- Maintain and manage the Master System Key for all manufactures of equipment approved to operate on the ALMR System.
- Program the physical System Key for requesting agencies with the necessary parameters, once the proper hardware is provided by the agency.
- Authorize the use of, or issue, the System Key software for those manufacturers who do not provide a physical System Key to authorized self-maintained member

agency technicians and/or to manufacturer-authorized service vendors that maintain equipment for ALMR agencies, as they become available, and upon request.
- Destroy the System Keys they manage, as they become obsolete.

2.5 User Agencies

The following conditions apply to any System Key or radio program developed for use by member agencies on any piece of equipment utilized on the ALMR System.

Agencies will:

- Agency designated “ALL” points of contact should request iButtons or System Keys via email through the ALMR Help Desk and are solely responsible for safeguarding/accountability
- Be responsible for acquiring/purchasing the proper programming software, hardware (iButton and iButton readers, or equivalent security device), and licenses necessary to program the subscribers they utilize, which utilize physical System Keys.
  NOTE: Some manufacturers charge a fee for their System Key software. When purchasing subscriber units, ensure you are aware whether or not the manufacture charges for the initial software and/or update software.
- Not distribute, disclose to or permit any unauthorized party to view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with or otherwise compromise the security of any codeplug programming file, System Key file, System IDs, encryption key file, template or talkgroup information for any agency on ALMR, for any reason.
- Immediately notify the ALMR Help Desk of a security breach in the event they learn that any party has improperly or fraudulently obtained any radio codeplug file, System Key, System ID, encryption key, template or talkgroup information.
- Be responsible for the cost of all reprogramming necessary to overcome said breach and be subject to sanctions, including loss of programming authorization, if determined to be at fault.
- Destroy manufacturer System Keys as they become obsolete, or when directed to do so by the OMO or SMO.
- Be prepared to replace all System Key hardware, which will be programmed to expire every three years.
- Provide an audit report for System Key hardware/software to the SMO every year showing location and who has possession/access
- Program only their own subscribers or those of agencies for which they are authorized to provide subscriber maintenance.
- Program all subscriber units to allow "Radio Inhibit" from the System Network Management Terminal (NMT).

- Program all subscriber units for write-protect file access only, if the equipment supports the write-protect function.
- Archive the file from the radio prior to shipping any radio to the vendor for repair **NOTE:** Radios may be sent with the programming intact. However, it is not permitted to ship radios to any vendor with encryption keys intact.
- Verify radios for correct codeplug information and that they are write protected, if capable, when returned from vendor repair.
- Maintain current and accurate records of all programming (i.e. fleetmapping) performed; codeplugs and subscriber units are subject to audit by the SMO.

	P25 FLEETMAP DOCUMENT
Customer Name	
Date Last Updated:	
TRUNKED SYSTEM DATA	**Documents the System ID, WACN ID, Control and Voice Channel Frequencies, etc**
SECURITY GROUPS & RANGES	**Documents Security Group names, Talkgroup/Multigroup/Agency Group range numbers and Individual Radio ID ranges**
TALKGROUPS & MULTIGROUPS	**Documents TG/MG/AG names and their operational features**
MULTIGROUPS vs. TALKGROUPS	**Documents which Talkgroups are mapped to which Multigroups**
AGENCY GROUPS vs. MULTIGROUPS	**Documents which Multigroups are mapped to which Agency Groups**
ENCRYPTION KEY PLAN	**Documents the Encryption Key numbers and strings**

NOTE: Please contact the ALMR Help Desk for a complete copy of the P25 Fleetmap document, if needed.

2.6 Vendors

Vendors provide a valuable resource for many agencies operating on the ALMR System through their subscriber maintenance services. Therefore, vendors are also responsible for following the policies and procedures established to maintain the security and integrity of ALMR and those agencies who utilize it.

Vendors will:

- Be responsible for acquiring/purchasing the proper programming software, hardware (iButton and iButton readers, or equivalent security device), and licenses necessary to program the subscribers they support, which utilize physical System Keys.
- Not distribute, disclose to or permit any unauthorized party to view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with or otherwise compromise the security of any codeplug programming file, System Key file, System IDs, encryption key file, template or talkgroup information for any agency on ALMR, for any reason.
- Immediately notify the ALMR Help Desk of a security breach in the event they learn that any party has improperly or fraudulently obtained any radio codeplug file, System Key, System ID, encryption key, template or talkgroup information.

- Be responsible for the cost of all reprogramming necessary to overcome said breach, and subject to sanctions, including loss of programming authorization, if determined to be at fault.
- Destroy manufacturer System Keys as they become obsolete, or when directed to do so by the OMO or SMO.
- Be prepared to replace all System Key hardware, which will be programmed to expire every three years.
- Provide an audit report for System Key hardware/software to the SMO every year showing location and who has possession/access.
- Program only their own subscribers or those of agencies for which they are authorized to provide subscriber maintenance
- Program all subscriber units to allow "Radio Inhibit" from the System Network Management Terminal.
- Program all subscriber units for write-protect file access only, if the equipment supports write-protect function.
- Verify for correct codeplug information and that they are write protected before returning to the agency.
- Maintain current and accurate records of all programming (i.e. fleetmapping) performed; codeplugs and subscriber units are subject to audit by the SMO.

	P25 FLEETMAP DOCUMENT
Customer Name	
Date Last Updated:	
TRUNKED SYSTEM DATA	Documents the System ID, WACN ID, Control and Voice Channel Frequencies, etc
SECURITY GROUPS & RANGES	Documents Security Group names, Talkgroup/Multigroup/Agency Group range numbers and Individual Radio ID ranges
TALKGROUPS & MULTIGROUPS	Documents TG/MG/AG names and their operational features
MULTIGROUPS vs. TALKGROUPS	Documents which Talkgroups are mapped to which Multigroups
AGENCY GROUPS vs. MULTIGROUPS	Documents which Multigroups are mapped to which Agency Groups
ENCRYPTION KEY PLAN	Documents the Encryption Key numbers and strings

NOTE: Please contact the ALMR Help Desk for a complete copy of the P25 Fleetmap document, if needed.

3.0 Compliance

Compliance with the System Key Usage Procedure is outlined in ALMR System Key Usage Policy Memorandum 400-16.