Alaska Land Mobile Radio Communications System

System Account Control Procedure 400-4

Version 10

December 27, 2018

Developed in conjunction with:

Table of Contents

Document Revision History ..... **ii**
Acronyms and Definitions ..... **iii**
1.0 Purpose **1**
2.0 Roles and Responsibilities **1**
2.1 Executive Council 1
2.2 User Council 1
2.3 Security Manager 1
2.4 System Management Office 2
2.5 User 2
3.0 Account Management **2**
3.1 New User Accounts 2
3.2 Privileged User Accounts 3
3.3 Default Accounts 4
3.4 Group Accounts 4
3.5 Password Maintenance 5
3.6 Inactive Accounts 5
3.7 Closed Accounts 5
4.0 Remote Access **6**
5.0 Training **6**
5.1 User Training 6
5.2 Materials 6
5.3 Exam Results 6
6.0 Compliance **7**

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	2/2/2009	Approved by the User Council – Final.	1
Shafer, Sherry	3/5/2010	Annual review. Approved by the User Council – Final.	2
Shafer, Sherry	8/23/2010	Annual review. Approved by the User Council – Final.	3
Shafer, Sherry	9/13/2011	Annual review. Approved by the User Council – Final.	4
Shafer, Sherry	8/30/2012	Annual review. Approved by the User Council – final.	5
Shafer, Sherry	11/15/13	Annual review/update; approved by the User Council - final.	6
Shafer, Sherry	12/2/2014	Annual review/update; approved by the Operations Management Office - final.	7
Shafer, Sherry	12/22/2015	Annual review/update. Approved by the Operations Management Office - final.	8
Shafer, Sherry	12/28/2016	Annual review/update. Approved by the Operations Management Office - final.	9
Shafer, Sherry	12/27/2018	Annual review/update. Approved by the Operations Management Office - final. 12.27.18 Dee Smith	10

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).

Cybersecurity formerly Information Assurance (IA): information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA and cybersecurity will be used interchangeably.

Information Systems Security Manager (ISSM): the individual responsible for establishing and maintaining security controls that ensure the availability, confidentiality and integrity of the ALMR System under the RMF.

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.

Risk Management Framework (RMF) for DoD Information Technology (IT): A structured approach used to oversee and manage risk for an enterprise. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. Requires the completion of the Assessment and Authorization (A&A), formerly certification and accreditation (C&A), process which results in an Authorization Decision (AD). The system must be reauthorized no later than every three (3) years.

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

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.

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.

1.0 Purpose

This document serves as the guide for access to the Alaska Land Mobile Radio (ALMR) Communications System and provides the necessary steps to be taken and/or followed in the creation and maintenance of user accounts. Proper System user account control applies to all employees, contractors, sub-contractors, consultants, temporary employees and other personnel assigned to or utilizing ALMR equipment including hardware, firmware and software.

This procedure meets the minimum requirement for System Account Control as outlined in NIST SP 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations.

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 Account Control Procedure warrant such action.

2.2 User Council

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

2.3 Information Systems Security Manager

The Information Systems Security Manager (ISSM) shall:

- Assign security priorities and approve security standards based on the system security impact of MODERATE Confidentiality, MODERATE Integrity and MODERATE Availability
- Monitor all privileged user assignments to ensure separation of functions and compliance with personnel security criteria established in Department of Defense (DOD) 5200.2-R
- Identify specific user actions that can be performed on the information system without identification or authentication. (**NOTE:** If required, the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.)
- Develop, disseminate and periodically review/update the ALMR System Account Control Procedure to effectively address purpose, roles and responsibilities, training and compliance

2.4 System Management Office

The System Management Office (SMO) shall ensure that all procedures set forth in this document are implemented and automated, where appropriate. The SMO shall report any deviation from these procedures to the ISSM within one business day of discovery.

2.5 User

All user agency points of contact (POCs) shall:

- Maintain a current list of their agency users who require a System account on ALMR
- Provide the ALMR Help Desk a new list each time a change is made
- Ensure that each individual who requires account access to the ALMR System does so using a discrete individual user account
- Ensure group accounts (e.g. dispatch consoles) utilize a single set of login credentials for all users in a group
- Ensure that all ALMR System user account passwords are changed every 60 days and in accordance with paragraph 3.5. Additionally, POCs must ensure users understand passwords are:
  - Not to be shared, embedded in access scripts or stored on function keys
  - Not to be written down, but instead committed to memory
  - Maintained in a confidential manner
- Notify the Help Desk immediately in the event that an ALMR user password is believed to be compromised

3.0 Account Management

At this time, the ALMR System has only two types of account holders - users and administrators.

A user is defined as any approved person assigned computing or communications assets for communicating on the ALMR System.

An administrator is defined as any approved person assigned access privileges at the administrative, system or root level, or with “super user” privileges that are used to modify the System.

3.1 New User Accounts

A request for a new user account or group account shall be submitted to the authorized agency POC, who will notify the ALMR Help Desk.

The request submitted by the agency POC should contain, for each user or group member:

- Name
- Title and position
- Organization
- Phone number
- Official email address
- Supervisor's name and contact information
- Projected transfer date (for military personnel)

3.2 Privileged User Accounts

A privileged user account gives the authorized user the ability to add, delete or modify records, or perform tasks consistent with administrative privileges.

An administrative account is a form of privileged user resulting in the authorized user's capability to control the ALMR System at the "admin" or "root" level. Administrative account access shall be limited to those individuals known to the ALMR System Manager, as approved by the ISSM.

3.2.1 Protection of Privileged User Accounts

Privileged user account passwords shall not be entered into unsecured clear text services. Examples of these services include, but are not limited to:

- FTP
- HTTP
- RSH
- Email
- Spreadsheets
- Plain language documents

Privileged user account passwords shall not be entered into fields, which are not masked on the screen. Privileged user account passwords shall not be stored on the System with a "remember me" option, password caching or any variation of such unencrypted storage. Any storage of privileged user account passwords will be protected by encryption conforming to DOD standards.

ALMR components will automatically terminate a user session after a pre-determined period of inactivity. Period length will be based upon functional requirements at the discretion of the ISSM.

3.2.2 Rights and Use of Privileged User Accounts

The SMO shall ensure that privileged user account permissions allow access to only that data, control information, software, hardware and firmware for which they are authorized access and have a need-to-know.

The SMO shall ensure that each privileged user with information assurance (IA) responsibilities (e.g. system administrator), in addition to satisfying all responsibilities of an authorized user, shall:

- Configure and operate technology according to ALMR information system policies and procedures and notify the ISSM of any changes that might adversely impact the security posture of the ALMR
- Establish and manage authorized user accounts for DOD information systems, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed

Assignment to privileged user roles with IA management access shall be made in accordance with the Privileged User Acceptable Use Procedure 400-7.

3.2.3 Privileged User Password Creation

The initial password for a privileged user shall conform to password complexity requirements (see paragraph 3.5). When a password is issued for maintenance personnel, it shall be the responsibility of the ISSM to ensure the password is reset or disabled across the ALMR System once maintenance is completed.

3.2.4 Privileged User Password Distribution

During distribution to the privileged user, the password will be protected to the same degree as the information to which the password provides access. The password of each privileged user account shall not be distributed to any user other than the designated account owner.

3.3 Default Accounts

Default accounts and associated passwords shipped with operating systems and/or application software will be removed or renamed prior to a new piece of equipment being installed on the ALMR network.

3.4 Group Accounts

Group accounts may be used when required to support system operations and missions. Each agency will establish and approve group accounts based on operational

needs. Required group accounts will be controlled by the SMO by performing the following activities:

- Assign individual group accounts and a unique password for individual groups
- Generate requested password resets
- Distribute the passwords to the POC securely
  NOTE: The agency authorized POC will be responsible for distributing the password to members of a group account
- Ensure that log records are maintained, which will enable identification of individuals with System access using group account credentials by user name, console name (for dispatch centers with multiple consoles), date and time

3.5 Password Maintenance

Passwords are required to be changed every 60 days. All passwords:

- Must be at least 15 characters long
- Cannot exceed 64 characters
- Must have the following characteristics:
  - At least one lower case alphabet (a-z)
  - At least one upper case alphabet (a-z)
  - At least one digit (0-9)
  - At least one of the following special characters:
    ~ ` ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ’ ” \ | , < . > / ?

At least four characters must be changed when a new password is created to replace an expired password.

NOTE: System mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse.

Passwords shall not be shared with any other personnel or disseminated in any way. The confidentiality of each password is the responsibility of the user to whom the password is assigned.

3.6 Inactive Accounts

Accounts that have been inactive for 90 days or more will be disabled until the requirement for further use is validated. Additionally, the SMO will immediately disable any account through which unauthorized user activity has been detected.

3.7 Closed Accounts

Users and supervisors are required to notify their respective authorized agency POC who, in turn, will notify the SMO when a user no longer requires access to ALMR. The

subject account will be deleted within two days of notification. In the case of a group account, the password will be reset and provided to the authorized agency POC.

4.0 Remote Access

The only form of remote data access allowed on the ALMR System network is the current external virtual private network (VPN) connection established for network and intrusion detection monitoring for the ALMR System. This capability is currently under contract to Motorola®, through the Motorola® Service Solutions - System Support Center (SSC).

ALMR System security hardening through migration to 7.13 has allowed for VPN access for Motorola® and SMO Technologists. This capability will allow System support personnel to monitor and maintain the ALMR System remotely.

Any other remote data connections to the ALMR network are specifically disallowed.

5.0 Training

5.1 User Training

All ALMR System users, at any level, shall be provided annual training and awareness on matters of account control. Ensuring ALMR System confidentiality, integrity and availability are prudent account control practices.

5.2 Materials

Training materials, and an examination, shall be provided by the SMO. The depth and length of this examination shall be defined by the ISSM.

The results of each examination must reflect satisfactory completion and will be maintained in accordance with the ALMR Records Management Procedure 300-1.

DOD personnel may satisfy this requirement by providing documentation of their DOD IA training, at least annually.

5.3 Exam Results

The ISSM shall review examination certificates, identify issues within the curriculum, address and manage reported issues identified under the scope of environmental and physical security related issues, and report violations of this procedure. The ISSM shall document all findings, and any recommended actions to be taken in the form of a sanction, and provide them to the UC.

The UC shall review the issue(s), and forward their recommendation(s) to the EC for approval/implementation.

6.0 Compliance

Compliance with the System Account Control Procedure is outlined in ALMR System Account Control Policy Memorandum 400-4.