



A FEDERAL, STATE AND MUNICIPAL PARTNERSHIP

Alaska Land Mobile Radio Communications System

System Account Control Procedure 400-4

Version 4

September 13, 2011

Developed in conjunction with:



Bering Straits Information Technology, LLC

A Subsidiary of the Bering Straits Native Corporation



Table of Contents

Table of Contents	i
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 Information Assurance Officer	1
2.4 System Management Office	2
2.5 Security Manager.....	Error! Bookmark not defined.
2.6 User	2
3.0 Account Management	2
3.1 New User Accounts	3
3.2 Privileged User Accounts.....	3
3.3 Default Accounts.....	4
3.4 Inactive Accounts.....	5
3.5 Group Accounts	5
3.6 Closed Accounts.....	5
4.0 Remote Access.....	5
5.0 Training	5
5.1 User Training	5
5.2 Materials	5
5.3 Exam Results.....	6
6.0 Compliance	6



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



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 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.

Executive Council: the ALMR Executive Council which is made up of members and associate members from the State of Alaska representing state agencies, the Alaska Municipal League, the Alaska Federal Executive Association, the Department of Defense – Alaska, and the Municipality of Anchorage.

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.

IAO: Information Assurance Officer

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

Mission Assurance Category (MAC): designation used to determine requirements and availability of information systems

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of approximately 278,000. 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.

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



*Alaska Land Mobile Radio Communications System
System Account Control Procedure 400-4*

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

User/Member: 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 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 ALMR and the necessary steps to be taken/followed in the creation/maintenance of user accounts. Proper System user account control applies to all employees, contractors, consultants, temporary employees, and other personnel assigned to utilize the Alaska Land Mobile Radio (ALMR) Communications System equipment including hardware, firmware, and software.

This procedure meets the minimum requirement for System Account Control as outlined in DOD Instruction 8500.2, Information Assurance (IA) Implementation.

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 Policy & 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 revisions hereafter.

2.3 Information Assurance Officer/Security Manager

The Information Assurance Officer (IAO)/Security Manager shall:

- Assign security priorities and approve security standards based on Mission Assurance Category II – SENSITIVE
- Monitor all privileged user assignments to ensure separation of functions and compliance with personnel security criteria established in DOD 5200.2-R and DOD Instruction 8500.2, Section E3.4.7
- Identify specific user actions that can be performed on the information system without identification or authentication. 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 Security Manager or IAO within one business day of discovery.

2.5 User

All user agency Points of Contact (POCs) shall:

- Maintain a current list of users who require a System user account on the ALMR System
- Provide the ALMR Help Desk a new list each time a change to the list 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:
 - A case sensitive, eight-character mix of upper- and lower-case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created to replace an expired password. System mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse.
 - Not be shared, embedded in access scripts, or stored on function keys.
 - Not be written down, but instead committed to memory
 - Maintained in a confidential manner (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)
 - Notify the Help Desk immediately in the event that an ALMR user password is believed to be compromised, user agency personnel

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 ALMR personnel assigned computing or communications assets for communicating on the ALMR System. A user account does not allow administrative access on any System component nor does it allow any modifications to the System. An administrator is defined as any approved ALMR personnel 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 to 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 allows a user the ability to add, delete, modify records, or perform tasks consistent with administrative privileges. A privileged user is a user with the authority to access a privileged user account. 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 IAO/Security Manager.

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 Security Manager.

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 for access and have a need-to-know.

The SMO shall ensure that each privileged user with 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 IAO of any changes that might adversely impact IA (DOD Instruction 8500.2, Section 5.11.1)
- 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 (DOD Instruction 8500.2, Section 5.11.2)

Assignment to privileged user roles with IA management access shall be according to “Investigative Levels for User with IA Management Access to DOD Unclassified Information Systems” Appendix Table E3.T1 (DOD Instruction 8500.2, Section E3.4.8)

3.2.3 Privileged User Password Creation

The initial password for a privileged user shall conform to password complexity requirements. When a password is issued for maintenance personnel, it shall be the responsibility of the IAO/Security Manager 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 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.

3.5 Group Accounts

Group accounts may be used when required to support system operation and mission. 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. The agency POC will be responsible for distributing the password to members of a group account.
- Distribute the passwords to the POC securely
- 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

3.6 Closed Accounts

Users and supervisors are required to notify their respective agency POC(s) who, in turn, will notify the SMO when a user no longer requires access to the ALMR network. 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 connection established for network and intrusion detection monitoring for the ALMR System. This capability is currently under contract to Motorola[®], through the Motorola[®] Security Operations Center. 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



Alaska Land Mobile Radio Communications System System Account Control Procedure 400-4

Training materials, and an examination, shall be provided by the SMO. The depth and length of this examination shall be defined by the IAO/Security Manager. 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 DOD IA training at least annually.

5.3 Exam Results

The IAO/Security Manager 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 policy. The IAO/Security Manager 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 Executive Council for approval.

6.0 Compliance

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