Alaska Land Mobile Radio Communications System

Privileged User Acceptable Use Procedure 400-7

Version 9

August 6, 2018

Developed in conjunction with:

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Huls, Chad	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	4/05/2011	Annual review/update. Approved by the User Council - final.	3
Shafer, Sherry	7/10/2012	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	7/30/2013	Annual review/update. Approved by the User Council - final.	5
Shafer, Sherry	7/29/2014	Annual review/update. Approved by the Operations Management Office – final.	6
Shafer, Sherry	8/5/2015	Annual review/update. Approved by the Operations Management Office – final.	7
Shafer, Sherry	8/12/2016	Annual review. Approved by the Operations Management Office – final.	8
Shafer, Sherry	8/6/2018	Annual review. Approved by the Operations Management Office – final.	9

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.

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Department of Administration (DOA): a State of Alaska (SOA) department that maintains the SOA Telecommunication System (SATS) and provides information technology (IT) and communications technical support to state agencies.

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).

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 Manager: the Operations Manager represents the User Council interests and makes decisions on issues related to the day-to-day operation of the system and any urgent or emergency system operational or repair decisions. In coordination with the User Council, the Operations Manager establishes policies, procedures, contracts, organizations, and agreements that provide the service levels as defined in the ALMR Service Level Agreement.

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

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.

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

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: 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 procedure defines terms and conditions for privileged users operating on the Alaska Land Mobile Radio (ALMR) Communications System according to the classification level of information to which they have been granted access. Access levels for ALMR are set forth by Department of Defense Instruction (DODI) 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, and DODI 8500.01, *Cybersecurity*.

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 Privileged User Acceptable Use Procedure warrant such action.

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the Privileged User Acceptable Use Procedure, and any substantial revisions hereafter.

2.3 System Management Office

The System Management Office (SMO) shall inform the Security Manager and the Operations Manager of any suspect activities, System information compromises, training discrepancies, etc.

2.4 Security Manager

The Security Manager (SCM) shall:

- Ensure each privileged System user acknowledges understanding of this procedure through a signed copy of the ALMR Privileged User Acknowledgement and Consent Form (Appendix A)
- Make recommendations to the Operations Manager, UC and EC concerning sanctions against any user who violates the provisions outlined within this procedure

2.5 Privileged Users

All privileged users have the responsibility to safeguard ALMR against unauthorized or inadvertent modification, disclosure, destruction, denial of service and misuse of privileges, as defined in the following categories:

2.5.1 Access Terminal Operators

Access terminal operators are responsible for ALMR systems setup, maintenance and monitoring activities. This includes the Operations Management Office (OMO), SMO, other contractors, sub-contractors and user organization staff assigned these responsibilities. This user group poses the highest risk to ALMR and requires the highest level of technical training and annual refresher training to insure the System is not compromised.

Each user in this group shall:

- Configure and operate information assurance (IA) and IA-enabled technology according to Department of Defense (DOD) Information Systems (IS) IA policies and procedures and notify the SCM of any changes that might have an adverse impact on the System
- Establish and manage authorized user accounts for the ALMR System, including configuring access controls and removing authorizations when access is no longer needed
- Ensure users possess the appropriate background investigation commensurate with level of access granted and, where appropriate, have a signed non-disclosure agreement on file with the ALMR SCM
- Complete Annual Cybersecurity Awareness Training Level III and provide proof of completion to the SMO and their immediate supervisor
- Generate and protect passwords or pass-phrases (passwords should not be written down, but instead committed to memory, unless recording them is required by operational circumstances and the record document is secured)
- Use only authorized hardware and software on the ALMR System (users will not install or use any personally owned hardware, software, shareware or public domain software)
- Access only that data, control information, software, hardware and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized
- Not alter, change, configure or use operating systems, programs or information systems except as specifically authorized by the SMO
- Safeguard and mark with the appropriate classification level all information created, copied, stored or disseminated from the ALMR information systems
- Not disseminate ALMR System information to anyone without a specific need to know as verified by the SCM, or his/her assigned agent
- Not utilize provided information systems for commercial or financial gain, including, but not limited to, illegal activities
- Be subject to all US criminal, civil and administrative laws regulating appropriate use of government information systems
- Immediately report any suspicious output, files, shortcuts or System problems to the SMO and SCM

- Inform the SCM when access to the ALMR System is no longer required (e.g. completion of project, transfer, retirement, resignation, etc.)
- Not unilaterally bypass, strain or test cybersecurity mechanisms. If cybersecurity mechanisms must be bypassed, users shall coordinate the procedure and receive written approval from the SCM
- Address any questions regarding policy, responsibilities and duties to the SCM
- Understand that violation of this, or any security measure, could result in the loss of access privileges

2.5.2 Console Terminal Operators

Consoles terminal operators are responsible for staffing Emergency Operation Centers, Command Centers and Dispatch Center operations. This user group poses the second highest risk to ALMR and requires a high level of training and annual refresher training to insure the System is not compromised.

Each user in this group shall:

- Establish and manage authorized user accounts for the ALMR System, including configuring access controls and removing authorizations when access is no longer needed
- Ensure users possess the appropriate background investigation commensurate with level of access granted and, where appropriate, have a signed non-disclosure agreement on file with the ALMR SCM
- Complete Annual Cybersecurity Awareness Training Level II and provide proof of completion to the SMO and their immediate supervisor
- Generate and protect passwords or pass-phrases (passwords should not be written down, but instead committed to memory, unless recording them is required by operational circumstances and the record document is secured)
- Use only authorized hardware and software on the ALMR System (users will not install or use any personally owned hardware, software, shareware or public domain software)
- Access only that data, control information, software, hardware and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized
- Not alter, change, configure or use operating systems, programs or information systems, except as specifically authorized by the SMO
- Safeguard and mark with the appropriate classification level all information created, copied, stored or disseminated from the ALMR information systems
- Not disseminate ALMR System information to anyone without a specific need to know as verified by the SCM, or his/her assigned agent
- Not utilize provided information systems for commercial or financial gain, including, but not limited to, illegal activities
- Be subject to all US criminal, civil and administrative laws regulating appropriate use of government information systems

- Immediately report any suspicious output, files, shortcuts or System problems to the SCM
- Inform the System Manager when access to the ALMR System is no longer required (e.g. completion of project, transfer, retirement, resignation, etc.)
- Not unilaterally bypass, strain or test cybersecurity mechanisms. If cybersecurity mechanisms must be bypassed, users shall coordinate the procedure and receive written approval from the SCM
- Address any questions regarding policy, responsibilities and duties to the SCM
- Understand that violation of this, or any security measure, could result in the loss of access privileges

3.0 Acceptable Use

Privileged users must understand they have the primary responsibility to safeguard ALMR information. They also have the responsibility to protect the System from, and report, any unauthorized or inadvertent modification, disclosure, destruction, denial of service and misuse. Access to any ALMR resource is a revocable privilege and is subject to constant monitoring and security testing

3.1 Data Classification

All data on the System is deemed Controlled Unclassified Information (CUI), and as set forth in DOD Manual 5200.01 Vol 4, *DOD Information Security Program: Controlled Unclassified Information (CUI)*. For Official Use Only (FOUO) is highest level of CUI for voice and data traffic on the System.

3.2 Public Key Infrastructure Use

3.2.1 For the purposes of acceptable use for encrypted communications conducted on ALMR, Public Key Infrastructure (PKI) provides a secure computing environment utilizing asymmetric encryption (public/private-keys) and is used to encrypt information and verify the origin of the receiver.

3.2.2 Any access to PKI systems, encryption keys and other resources, in relation to the PKI used on the System, is privileged and is granted on an as-needed basis. ALMR users agree to ensure all PKI-related information and systems are safeguarded, and that no information is disclosed, or access given, to an unauthorized individual.

4.0 Compliance

Compliance with the Privileged User Acceptable Use Procedure is mandatory and is outlined in ALMR Privileged User Acceptable Use Policy Memorandum 400-7.

Appendix A
Privileged User Acknowledgement and Consent Form

I, _____, have read the ALMR Privileged
(Print Full Name)
User Acceptable Use Procedure 400-7, and accept the terms and conditions set forth therein. I give the ALMR Executive Council the right to use my personal information for the purpose of complying with US Federal Directives allowing me access to the ALMR network environment. I understand that if I violate the rules of this policy my access can be terminated and I may face disciplinary measures including administrative sanction or criminal prosecution.

_____
Name (Printed)

_____ _____
Signature Date

_____
ALMR Security Manager Signature