Alaska Land Mobile Radio Communications System

System Backup and Recovery Procedure 400-5

Version 19

March 17, 2025

Table of Contents

Document Revision History

Date	Reason for Changes	Version
12/22/2008	Approved by the User Council – Final.	2
3/1/2010	Annual review/update. Approved by the User Council – Final.	3
2/16/2011	Annual review/update. Approved by the User Council - final.	4
3/13/2012	Annual review/update; approved by the User Council - final.	5
3/4/2013	Annual review. Approved by the Operations Management Office - final.	6
3/5/2014	Annual review/update. Approved by the Operations Management Office - final.	7
3/24/2015	Annual review/update. Approved by the Operations Management Office - final.	8
3/18/2016	Annual review. Approved by the Operations Management Office - final.	9
3/3/2017	Annual review. Approved by the Operations Management Office - final.	10
3/14/2018	Annual review. Approved by the Operations Management Office - final.	11
4/3/2019	Annual review. Approved by the Operations Management Office - final.	12
4/27/2020	Annual review. Approved by the Operations Management Office - final.	13
3/23/2021	Annual review. Approved by the Operations Management Office - final.	14
3/21/2022	Annual review. Approved by the Operations Management Office - final.	15
3/8/2023	Annual review. Approved by the Operations Management Office - final.	16
9/19/2023	Out of cycle review for security update. Approved by the Operations Management Office - final.	17
3/6/2024	Annual review. Approved by the Operations Management Office - final.	18
3/17/2025	Annual review. Approved by the Operations Management, System Management, and Security Manager Offices – final.	19

Acronyms and Definitions

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

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, as established in the Cooperative and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents 165 cities, boroughs, and unified municipalities.

Alaska Public Safety Communication Services (APSCS): a State of Alaska (SOA) office in the Department of Public Safety (DPS) that operates and maintains the SOA Telecommunications System (SATS) supporting ALMR and providing public safety communication services and support to state agencies.

Cooperative and Mutual Aid Agreement: the instrument that establishes ALMR and sets out the terms and conditions by which the system will be governed, managed, operated, and modified by the parties signing the agreement.

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

Department of Public Safety (DPS): a State of Alaska (SOA) department where the SOA Telecommunications System (SATS) and ALMR programs reside.

DODI: Department of Defense Instruction

Executive Council: governing body 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-DD agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage).

FV: FullVision® INM Database Server

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.

Key Management Facility (KMF): allows for secure re-keying of radios over the air.

Member: a public safety agency including, but not limited to, a general government agency (local, state, tribal, 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.

Network Attached Storage (NAS): is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity.

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.

State of Alaska (SOA): the primary maintainer of the State's infrastructure system, and shared owner of the system. The State of Alaska sponsors local/municipal agencies onto 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.

SSS: System Statistics Server

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. All terms and conditions of the Cooperative and Mutual Aid agreement defined apply to local/municipal government agencies that are sponsored/represented by the State of Alaska.

User Council: governing body 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 operation plans, procedures, and policies.

UCS: User Configuration Server

ZDS: Zone Database Server

ZSS: Zone Statistics Server

1.0   Purpose

This procedure defines required actions to be taken by the System Management Office and Operations Management Office personnel for performing any required ALMR system backup and recovery operations.

This procedure meets or surpasses the minimum accepted level of preparedness for backup and recovery for Alaska Land Mobile Radio (ALMR) systems in the form of technical, operational, and managerial control as required under NIST SP800-53r5, *Security and Privacy Controls for 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 Backup and Recovery Procedure warrant such action.

2.2   User Council

The User Council (UC) shall be responsible for:

- Formal approval of the System Backup and Recovery Procedure, and any substantial revisions hereafter.
- Reviewing all notices of violations and the recommended actions, in the form of sanctions to be implemented, as provided by the Information Systems Security Manager, prior to submittal to the EC.

2.3   Operations Management Office

The Operations Management Office (OMO) is responsible for:

- Briefing the UC and the EC of violations pertaining to system backup and recovery, when notified by the ISSM.
- Verifying and documenting backups are being completed (daily, weekly, or as needed).
- Verifying and documenting the operating system media and other critical software is stored, as required.
- Verifying a master list of ALMR hardware and software components exists and is stored, as required.
- Ensuring backup and recovery procedures are tested annually and advising the UC and EC of the results.

2.4 System Management Office

The System Management Office (SMO) shall coordinate and oversee all backup and recovery operations. This includes, but is not limited to:

- Maintenance and backup of an ALMR hardware asset baseline.
- Access control and storage of all ALMR backup media.
- Scheduling and performance of critical system backups.
- Coordination of recovery efforts during a system disaster or incident.
- Training of all personnel responsible for backup and recovery procedures.

2.5 Information Systems Security Manager

The Information System Security Manager (ISSM) shall be responsible for:

- Developing, disseminating, and periodically reviewing/updating formal documented procedures that address the purpose, scope, roles and responsibilities, and compliance with system backup and recovery.
- Facilitating the implementation of the backup and recovery procedures, if/when required.
- Managing reported issues identified under the scope of the System Backup and Recovery Procedure.
- Reporting violations to the OMO.
- Documenting any actions to be taken in the form of a sanction and forwarding those actions, through the OMO, to the UC for review, and then to the EC for approval.

3.0 System Baselines

The SMO will maintain a compiled list of all ALMR hardware and software components. Motorola® provides this list as a service whenever a major change is made to the system. The list provided by Motorola® will be used as the basis for system recovery prioritization, as discussed later in this document (para 7.3). A backup copy of this inventory shall be stored in a fire-rated container and not located on site with the original list.

The baseline will include the following items regarding each piece of hardware:

- Manufacturer
- Type
- Model
- Physical location
- Network topology/architecture

The baseline will include the following items regarding each piece of software:

- Manufacturer
- Type
- Version
- Software license number(s)
- User manuals
- Procedures

The SMO will be responsible for ensuring that new/upgraded hardware or software added to the ALMR system is documented within the baseline and a new backup copy of the list is produced and stored, accordingly.

4.0 Backup Requirements

Backup operations will be implemented in a way that minimizes impact on the network and system resources.

4.1 Daily Backups

4.1.1   Backups are performed daily using an incremental process that is scheduled in the Backup Server (BKUP01) and used as the main backup library. On the first workday of the week, all backup data is manually moved via the BAR Server to the "offsite" Network Attached Storage (NAS). These devices are configured at system development to automatically perform incremental backups daily and are no longer managed by technicians. The following device backups are moved in each Zone.

- System and Zone Domain Controller – UCS-DC01/DC01
- User Configuration Server - UCS01.UCS
- Internet Protocol Capture 1 and 2 – IPCAP01/02Zone Statistical Server – ZSS01
- Unified Event Manager UEM01
- Core Security Management Server – SZ014201.UCS
- Zone Database Server - ZDS01
- Air Traffic Router ATR01
- Bar Server – BKUP01
- License Manager – LM01Zone Controller 1 and 2 – ZC01/02
- Loghost01
- Packet Data Gateway Router - PDR01
- Unified Network Configurator - UCS-UNC01
- System Statistical Server – SSS01

4.1.2   A copy of the documents on the network share server and CommShop 360 are backed up by the State of Alaska nightly.

4.2   Weekly Backups

A backup of all ALMR controlled Key Management Facility (KMF) server databases shall be performed at least weekly.

4.3   As-Needed Backups

All network device configurations shall be backed up before and after ALMR system changes. This includes, but is not limited to, domain controllers, routers, firewalls, and switch configurations.

4.3.1   System Change/Update Backup

A system backup, to include system status data, will be created before any major system changes are enacted or before any system updates are performed. The backup will be retained in the designated offsite location for at least five working days after the changes.

After changes have been completed, and a successful reboot has been accomplished, the regular backup schedule shall be resumed.

4.3.2   Maintenance of System Log Files

Security event logs are maintained for a year. System data and logs are backed up to the NAS, where it is kept for the appropriate length of time. The two Zones act as mirrored sites for each other. In the event of a catastrophic failure, the other Master Site can be configured to handle the traffic from the failed Master Site and can also be used to recreate the failed Master Site.

5.0   Media Labeling

Files on the backup server are labeled electronically with the appropriate data to allow the content to be quickly found.

6.0   Backup Storage

Back-up copies of the original media of the operating system and other critical software shall be stored in a fire-rated container and not located on site with the original operational software.

This material will be stored within a secure area that is restricted to authorized individuals only.

6.1   Designated Storage Locations

The following designated storage location(s) are approved for all system backup media.

ALMR System Location	Backup Media Storage Location
Zone 1 Master Site Anchorage, AK	Anchorage, AK
Zone 2 Master Site Fort Wainwright, AK	Fort Wainwright, AK

Table 6-1. Designated Storage Locations[1]

6.2   Transfer to Off-Site Storage

Backup data is transferred to designated storage locations on a weekly basis by the SMO.

7.0   Recovery Procedures

7.1   Recovery Documentation and Procedures

All backup and recovery operations shall follow the documented procedure, which is specific to the backup software used and tailored to the data that is being backed up.

7.2   Secure Recovery

7.2.1   The hardware and software used by ALMR personnel for backup and recovery of the ALMR system shall be protected from unauthorized access or modification with the same diligence that is applied to the ALMR system itself.

7.2.2   If appropriately cleared personnel, as defined by the ISSM, are unavailable to perform maintenance or repair, personnel with a lesser clearance may be used. For the duration of the recovery/repair, maintenance personnel shall be escorted and monitored by approved ALMR personnel, as defined by the ISSM.

7.2.3   If at any point during the resumption of the system, a situation is encountered which could inhibit a trusted recovery, ALMR personnel will cease resumption activities, document the situation, and consult with the ISSM. It is the responsibility of the ISSM to determine the appropriate mitigating procedures necessary to enable a trusted recovery of the system. The ISSM shall maintain the original documented information of the incident and provide a copy to the Operations Manager.

---

[1] Exact physical locations are not listed for security reasons.

7.3 Prioritization of Recovery

If recovery is required on multiple systems, priority groups have been established to guide the recovery of the systems. Systems in Priority Group 1 should be recovered first, and then Priority Group 2 next, and continuing until all systems are restored.

A current prioritized system recovery list can be found at Attachment 1, Restoration Priority Worksheet.

7.4 Required Recovery Personnel

The SMO will be available to respond (24/7) upon system failure notification and shall coordinate emergency maintenance support for key information technology assets.

8.0 Backup and Recovery Procedure Testing

Backup and Recovery procedures for the ALMR system shall be tested annually by the SMO, and all results of the test shall be recorded and provided to the Operations Manager.

9.0 Training and Awareness

All personnel responsible for recovery of the ALMR system shall receive appropriate training specific to their roles in the backup and recovery processes.

10.0 Compliance

Compliance with the System Backup and Recovery Procedure is outlined in ALMR System Backup and Recovery Policy Memorandum 400-5.

Attachment 1
Restoration Priority Worksheet

Element	Restoration Priority Group	Zone or Site
Air Traffic Router - Virtualized	1	Zone
Alerting Master Computer		
Backup and Recovery Server - Virtualized		Zone
Border Gateway	2	Zone
CCGW		
Centralized Event Logging Server - (SYSLOG Server) - Virtualized		Zone
Core Backhaul LAN Switch- 2620-24		
Core LAN Switch-3800	1	Zone
Core Router	1	Zone
Core Security Management Server (CSMS) - Virtualized	1	Zone
Corporate WAN Router (CWR) (patch/ relay panel)		Zone
DAS_01		
Domain Controller - Virtualized	1	Zone
Exit Router	1	Zone
Firewall Management Server - Virtualized	2	Zone
FSA4000 FEP		
FSA4000 RTU		
GPB 8000 Reference Distribution Module (RDM)		
Graphical Master Computer - Virtualized		Zone
Graphical Workstation		
IDS LAN Switch-2620		
IP PBX Server	4	Zone
IP Simulcast Remote Site Gateway		
IV&D Router		
Juniper Firewall ISG1000	2	Zone
Juniper Firewall SSG140	2	Zone
KMF Client		
KMF CryptR		
KMF Server		
KVL 4000		
MCC 7500 Aux I/O Server		
MCC7500 Archiving Interface Server (AIS)		
MCC7500 Dispatch Console		
MCC7500-E Disptach Console		
Media Gateway		
Mediation LAN Switch-2620		
MRV Terminal Server LX4008t		
MRV Terminal Server LX4048t		
Network Time Server		
NICE IP Logger		
NICE Replay Workstation		
NM Client - Standalone	5	Zone
NM-Dispatch Router	5	Zone

Element	Restoration Priority Group	Zone or Site
NM-Disp-Conv LAN Switch-2620	5	Zone
Packet Data Gateway – IVD – Virtualized		Zone
Peripheral Network Gateway		
PN Router	2	Zone
PN Server	2	Zone
Prime Site Router (IP Simulcast Prime Site Router)		
Raymar Modem (model TEL-6209548200010)		
Remote LAN Switch JL253A HP2930-24		
Remote Simul Router		
Remote Site – GCP 8000 – Site Controller (CommonSC)		Site
Remote Site – PSC9600 – Site Controller (PSC)		Site
Remote Site 700 – GTR 8000 – Site Repeater (SR)		Site
Remote Site Access Gateway (Ethernet Links only)		Site
Remote Site VHF – GTR 8000 – Site Repeater (SR)		Site
Remote Site VHF – Quantar – Site Repeater (SR)		Site
SDM3000 Network Translator		
SDM3000 RTU		
Simul Backhaul LAN Switch-2620		
Simul Prime LAN Switch-2620		
Simul Prime LAN Switch-2650		
Simul Remote LAN Switch-2620		
Simulcast – ASTROTAC9600 – Comparator		
Simulcast – GCM 8000 – Comparator		
Simulcast – GCP 8000 – Site Controller (SSC)		
Simulcast 700 – GTR 8000 – MultiSite Base Radio (MSBR)	1	Site
Simulcast UHF – Quantar – MultiSite Base Radio (MSBR)	1	Site
Simulcast VHF – GTR 8000 – MultiSite Base Radio (MSBR)	1	Site
Simulcast VHF – Quantar – MultiSite Base Radio (MSBR)	1	Site
Site Gateway	1	Site
Site Gateway (Console Site)	1	Site
Site Gateway (Conventional Channel Interface)	1	Site
Site Gateway (IP Simulcast Prime Site)	1	Site
System Statistical Server – Virtualized	1	Zone
Telephone Media Gateway (TMG)	4	Zone
TeNSr Channel Bank Model 600	1	Site
TeNSr Channel Bank Model 800	1	Site
Unified Event Manager – Virtualized	1	Zone
Unified Network Configurator – Virtualized	1	Zone
User Configuration Server – Virtualized	1	Zone
Virtual Server – DL 360 G6	1	Zone
Virtual Server – VMS01	1	Zone
Virtual Server – VMS02	1	Zone
Virtual Server – VMS05	1	Zone
Virtual Server –(ESX Server)– DL 360	1	Zone
Vortex VPM		
Z400 High Tier		
Z400 Low Tier		
Z400 Mid Tier		
Z420 High Tier		
Z420 Low Tier		
Zone Controller – Virtualized	1	Zone
Zone Database Server – Virtualized	1	Zone