



Alaska Land Mobile Radio Cybersecurity Policy

1. Applicability

This policy applies to all member agencies, employees, contractors, subcontractors, consultants, temporary employees, and other personnel assigned to or utilizing the Alaska Land Mobile Radio (ALMR) Communications System. Any substantial revision or update of this policy must be approved by the User Council.

2. Policy

This policy defines the cybersecurity standards applied to the ALMR system and by which all member agencies and support personnel shall abide. The ALMR system shall employ the use of Department of Defense (DOD), Federal, and Industry security guidelines and recommendations, and enforce all cybersecurity requirements for training, access controls, and acceptable use.

3. Procedures

All data on the system is deemed For Official Use Only (FOUO) and shall be treated as Controlled Unclassified Information (CUI) IAW DOD Manual 5200.01v4, *DOD Information Security Program: Controlled Unclassified Information (CUI)*. The System Management Office (SMO) shall implement a cybersecurity posture, which is sufficient to maintain an Authority to Operate (ATO), as defined by the Risk Management Framework (RMF) for DOD Information Technology (IT) and determined by the Alaskan Command J6 or DOD Approval Authority (AO). System users shall be knowledgeable of, and comply with, all applicable cybersecurity policies and training requirements, as outlined in Cybersecurity Procedure 200-5.

4. Effective Date

This policy shall become effective upon signature and shall remain in effect until rescinded. The policy shall be reviewed periodically and updated, as required.

Paul L. Fussey 8/3/2023

Paul Fussey
Operations Manager
Alaska Land Mobile Radio