



Alaska Land Mobile Radio System Account Control Policy

1. Applicability

This policy applies to all employees, contractors, sub-contractors, 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

The SMO shall establish and enforce the necessary account access controls to prevent exposure of the ALMR system to risks including attacks, compromise of network systems and services, legal issues, and the potential Denial of Authority to Operate under the Risk Management Framework (RMF) for DoD Information Technology (IT).

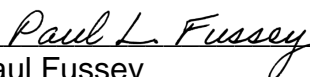
This policy meets or surpasses the minimum accepted level of system account access control for ALMR systems in the form of technical, operational and managerial control as required under DODI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)* and NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

3. Procedures

All account management including requests regarding the creation, modification, or deletion of an ALMR system user account or group account shall be overseen by the Systems Management Office (SMO). Additionally, only an agency's designated ALMR point of contact may request that a user account or group account be created or deleted. Appropriate management of system user accounts shall be performed in accordance with ALMR System Account Control Procedure 400-4.

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This policy shall become effective upon signature and shall remain in effect until rescinded.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 Fussey
Operations Manager
Alaska Land Mobile Radio