Transcript – ALMR Security Procedures

Welcome to this Alaska Land Mobile Radio training presentation, ALMR security procedures.

The Alaska Land Mobile radio system is a critical system for many agencies throughout the state, including many first responders at various levels, including local, state, federal and Department of Defense.

There are various security policies and procedures in place to ensure system security and comply with standards and regulations required for such a system. This training video will review the security responsibilities for all ALMR users.

The system is designed for maximum security and reliability. As such, ALMR is a closed system. That means that there is currently no part of the system that is connected to the Internet or any other type of system, except for those authorized for system maintenance and repair. The system also uses and meets all requirements for Department of Defense Computer Systems and is authorized specifically for use with DoD operations.

The security measures in place for the system include physical security as well as electronic security. Note that all activity that is conducted on the system is subject to monitoring and review.

All ALMR users have responsibility for the security of the system. Most users of ALMR do not have direct access to ALMR computer systems. However, each radio or subscriber unit that connects to the system contains sensitive information. This type of information could be potentially used for a malicious actor to gain control of the system or obtain security information. All users should take care to maintain control of their equipment at all times, especially portable and mobile radios and key loaders. If there is a lost or stolen ALMR connected device, such as a radio, it must be reported immediately to the system management office help desk. The help desk will assist with deactivating the radio and locking it out from any access to the system.

To ensure that your reporting is accurate, your agency must keep accurate records of the equipment that is connected to the ALMR system. Each radio has an ID number and a serial number. Be sure that you have accurate records of who has what unit with which ALMR ID and serial number to ensure that if such a situation were to occur, the correct unit can be deactivated and reported stolen or lost.

Lost or stolen equipment must be reported to law enforcement authorities after reporting to the system management office, they will file a report within the NCIC of the lost item.

System policy and procedure defines two levels of system users, level one and level two. Level 2 users are system management office technicians and others that have the responsibility for maintenance and upkeep of the system. The requirements for these users are set out in ALMR Policy and procedure, But are outside the scope of this training.

Level 1 users include individuals from agencies throughout the state at all levels of government, and these may include dispatchers and others who operate dispatch consoles, those that are points of contact from member agencies, as well as those that manage key management facilities throughout the system. These users have several responsibilities to ensure they maintain system security.

Password security is one of the easiest ways to help maintain security of the system. ALMR requires passwords be changed every 60 days, and there are complexity requirements for these passwords outlined in all of our policy. If there is suspect of any lost or compromised password, change that password immediately and report the incident to the help desk.

People with access to consoles must not install any software on these, including remote access technologies or other items that are not cleared by the ALMR system management office. Any type of external software or devices connected to consoles may pose a security risk.

Level 1 users are also required to complete annual cybersecurity training on these and other issues related to security of the system. The DoD Cyber Awareness Challenge is required for all Level 1 users annually.

Items such as why is cyber security necessary? Physical and electronic security acceptable? Use reporting and violations of the federal Risk management framework are among the many items reviewed in this computer-based training.

Additional items about general cyber security guidelines are also included. Some items may not directly correlate to the ALMR system, however they are good best practices for all types of essential systems that you may use in your day-to-day job.

The system management Office keeps records of those that have completed the cybersecurity training contact the Alamar helpdesk to report completion, or if you have any questions on this requirement.