MARRS System Subscriber Access Policy (11/2023)

Non-Public Safety Entities

The purpose of this document is to outline MARRS Policies regarding access for non-Public Safety entities, and to incorporate changes made with the adoption of AES Encryption.

The MARRS System is a coalition of the willing radio owners. MARRS was set up as a governance body to connect these different systems together. The voting members of MARRS are all radio system owners. In most cases, MARRS develops policies and guidance on issues that are regional (regional talk group usage, encryption standards, car chase channels, radio feature recommendations for use on MARRS and patching of channels). Coordination is also required because with the connection of the systems, it is possible for one owner's system resources to be negatively affected by another radio system owner's usage. All the systems are not the same size or capacity, and since they are connected, the larger systems can overtake the smaller systems available resources and create access issues for the smaller agencies.

Each subsystem (Master Sites and Prime Sites) is individually owned by the City or County Governments they operate in. The System Owners have a large financial investment in the infrastructure of their systems and are responsible for the maintenance and upgrades to keep all systems in sync. Each System Owner determines how these costs are funded, whether it is an appropriation by their individual local governments or sharing the costs with the users through subscriber fees. If the System Owners choose to charge subscriber fees, it is up to the System Owner to determine what that fee must be to cover the maintenance and upgrade costs. Subscribers are expected to pay these fees to access the radio system.

Ultimately, each Site System Owner has the decision-making authority over who is granted access to their system. A Site System Owner can allow access to an entity if they have the capacity to provide service without degrading the operation of existing subscribers, provided they meet all the following conditions:

1. Must be a tax funded entity. Private companies are not allowed access to the MARRS Public Safety System, with the exception of a company contracted to provide emergency services to a Subscriber Agency. Example 1: A private ambulance service contracted to provide emergency services to a member agency can be allowed access to the necessary resources to provide said services. They would not be allowed to access MARRS for other purposes and would have to come before the MARRS committees for approval prior to being granted access. Example 2: A Public School District can be allowed to access to the necessary resources for communications within their School District, provided those resources are owned by the Site System Owner the district is geographically located in. Additional System access must meet the conditions of Item (2).

2. Must not adversely affect the overall MARRS System resources, without the consent of all MARRS owners. A MARRS owner may give access to a qualifying entity to the resources of their Prime Site, but may not give access to resources of the other Prime Sites without the consent and approval of the affected Site Owners. This includes all Regional talkgroups.
3. In the event the qualifying entity desires access to the unencrypted Regional Assets, they must request access through the MARRS Committees, provide justification for the need to access them, and receive approval for use of the Regional Assets. Access to the Encrypted Regional talkgroups, and the System AES Encryption Key, is prohibited for non-Public Safety entities.
4. Talkgroups other than Regional assets belong to the subscriber agency. Only the talkgroup owner may grant permission for access to their private talkgroups. Written permission from the talkgroup(s) owner is required to allow access to other agencies talkgroups. For example, if a private ambulance has approval to operate on a Prime Site, the expectation of having access to talk groups of agencies on that site should not be assumed. In this example, Grandview fire may grant them access to a talk group belonging to Grandview Fire, but, they do not have access to a KCFD TAC t/g without permission in writing from KCFD.
5. Must comply with all Technical Specifications for equipment used on the MARRS System.
6. Must comply with all operational requirements and policies of the MARRS System, including policies on access to the MARRS AES System Encryption Key. Only Public Safety entities will be allowed access to the System AES Encryption Key. (A Private Ambulance Service contracted to provide emergency services to a member agency is considered to be operating as a Public Safety entity and would be allowed to access the System AES Encryption Key on talkgroups used by the member agency).
7. Must sign a user agreement with the Prime Site owner and comply with the terms of that agreement.