



Statewide Interoperability Radio Network (SIRN)

Standards, Protocols, Procedures



Document Section	5 – Use by Non-Governmental Agencies	Status: SIEC Sub Committee Approval Date: 5/24/2022 SIEC Approval: 5/24/2022
State Standard Number	5.1.0	
Standard Title	Non-Governmental Entities Eligibility and System Privileges	
Date Established		
Replaces Document Dated	N/A	
Date Revised/Reviewed	5/24/2022	

1. Purpose or Objective

The purpose of this Standard is to establish policy and procedure for use of the Statewide Interoperable Radio Network (SIRN) by entities not designated as a governmental public safety or public service agency. These entities include various private, support or educational organizations including but not limited to Disaster Relief Organizations (DRO), higher educational institutions, media agencies, and private hospital systems.

2. Technical Background

Capabilities

The SIRN platform has the capability to provide two-way trunked radio communications between two devices anywhere in the State including between third party non-governmental or private entities, which serve an essential purpose in the preservation of life and property.

Constraints

Unfettered access to SIRN can cause adverse effects. First, to preserve SIRN’s limited capacity, it is important to ensure that access to SIRN is the optimal method of communication for the agency that seeks access. Secondly, sensitive and mission critical information communicated by first responder agencies over SIRN must be protected from intentional or inadvertent compromise. Therefore, access privileges to SIRN must be provided in a controlled and coordinated manner.

3. Operational Context

Various use cases exist for SIRN access by non-governmental and private entities. Some examples include:

- Private hospitals systems with routine communications needs with public and private ambulance companies
- Disaster Relief Organizations (DROs), which serve critical support functions coordinating supplies, logistics, volunteers and relief services
- Education institutions with first responder courses (e.g., fire service training), which may provide first hand training on communications tools used by first responders

Each of these scenarios requires access to SIRN in a manner customized to serve the purpose and in compliance with this Standards.





Statewide Interoperability Radio Network (SIRN) Standards, Protocols, Procedures



4. Recommended Protocol/ Standard

Non-governmental Entity SIRN Access Eligibility

SIRN is generally accessible to any agency—public, private or quasi-governmental—that provides a function in the overall emergency response and mitigation ecosystem. Any entity may be approved by the North Dakota SIEC on a case-by-case basis; however, the following considerations shall be used to determine eligibility:

- Governmental, quasi-government, non-profit and private entities with an emergency service function
- Public Safety Agencies (Law Enforcement, Fire, Emergency Medical Services, Emergency Management, Public Safety Answering Points, Dispatch Centers)
- Public Utilities
- Public Service agencies
- Public Works
- Educational Institutions
- Hospital/Medical Institutions
- Public Health Agencies
- Disaster relief organizations
- Transit Agencies
- Private EMS

Talkgroup Assignments and Use

Entities that do not employ SIRN for their routine daily communications or do not have dedicated talkgroup(s) will typically be assigned talkgroups by the Incident Commander in coordination with the Public Safety Answering Point (PSAP), or a PSAP for the duration of their engagement in the event. Generally, one of more of the SIRN Statewide and Regional Talkgroups will be assigned for this purpose.

Entities with specific and unique needs may have dedicated talkgroups approved by the SIEC per their participation plan.

Programming Restrictions

The following programming restrictions apply:

- *Educational Institutions*: SIRN radios may be used to support courses geared toward first responders; radios used for such training may NOT be programmed with live public safety talkgroups. Educational institutions must request dedicated talkgroups for that purpose. This limitation does not apply to law enforcement agencies affiliated with educational institutions.





Statewide Interoperability Radio Network (SIRN) Standards, Protocols, Procedures



5. Recommended Procedure

Full Compliance

Non-governmental entities with access to SIRN shall comply with all SIRN usage standards including but not limited to standards on equipment type, device programming and user training.

Usage Limitations

Non-governmental entities are strictly limited to the communications privileges for which the agency is approved and is necessary. Internal day-to-day, administrative, and other non-purpose specific communications are not permitted.

Application Process

Entities and organizations seeking to obtain SIRN access shall follow the process below:

- Complete Participation Plan detailing:
 - the number and types of radios
 - the number of talkgroups requested
 - how and by whom the talkgroups will be used
 - how use of SIRN system aligns with the organizations Emergency Response Plan
- Obtain initial approval from the PSAP, followed by PSAP-to-CRIB to secure CRIB approval, and from the CRIB-to-subcommittee for review and approval, and then to the SIEC for final approval
- Enter into a system use memorandum detailing, among other things, an agreement to comply with the SIRN Standards and Standard Operating Procedures (SOPs)

Device Type and Maintenance Standards

Entities are responsible for maintaining, repairing, and programming their SIRN radios in accordance with all applicable standards.

Radio programming shall be done by a vendor approved in accordance with SIRN Standard 2.17.0 Technical Staff and Maintenance Providers Training and Qualifications.

6. Management

Non-governmental entities are responsible for all costs associated with compliance with this standard.

The SIRN Statewide Administrator shall manage the agreement process and maintain a list of organizations with devices with SIRN access and the level of access/privileges they have.