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

Document Section	**2 – Management of System**	**Status**: SIEC Sub Committee Approval Date: 6/28/2021
State Standard Number	**2.14.0**	
Standard Title	**Subscriber Programming System Keys**	
Date Established	**03/15/2021**	**SIEC Approval**: 6/28/2021
Replaces Document Dated	**NA**	
Date Revised/Reviewed	**NA**	

1. Purpose or Objective

The objective of this standard is to provide guidance for the proper management of radio programming "System Keys," which are used for programming subscriber radios with user-definable SIRN configuration data.

2. Technical Background

Capabilities

The North Dakota Statewide Interoperability Executive Committee (SIEC) wants to ensure that the highest level of security is incorporated into the North Dakota Statewide Interoperability Radio Network (SIRN) in order to protect the integrity of its users and the SIRN as a whole.

System Keys are electronic/hardware-based protection locks or utilities authenticating the use of programming software and system data to configure radios for SIRN access. Safekeeping and proper use of System Keys and corresponding radio programming software are critical to system integrity and security.

Both System (software file) and Advance System Keys (hardware-based) assist in issuing permissions to configure SIRN subscriber devices by allowing for the following protections:

- Restricting who is given access to program the radios and restricting radio and talkgroup IDs
- How long the key will be operable
- An extra layer of security for users as these keys are unable to be replicated

Security Options also vary by the radio brand the system user selects to access SIRN. For example, the radio might include an option to password protect the radio. This will allow the agency to prevent any modifications to the radio settings without inputting the password.

Constraints

The Statewide System Administrator has to manage and issue a wide variety of system keys to a large pool of radio technicians supporting subscribers from multiple vendors, each of which may have different configuration permissions.

Per the policies herein, the Statewide Administrator will typically obtain a configurable system key from

the radio programmer, manufacturer, or user, and will issue or configure unique keys with a specific set of electronic rights/permissions.

Approved System Key Users will have to sign for and will incur all the costs and liabilities associated with each key, absolving SIEC and its representatives of any liabilities and/or costs associated with its use or impact from use of the key.

3. Operational Context

Misuse or unauthorized duplication of System Keys can affect the integrity of SIRN. The wide range of system key options and configurability provided by subscriber vendors highlights the need for strict policy and procedure on the creation, distribution, and storage of System Keys.

Hardware Keys are strongly encouraged to increase security in the programming of the radios as well as protecting the integrity of SIRN.

4. Recommended Protocol/ Standard

- **General Standards**

  Do not program a radio you are not responsible for without written consent.

  System Keys shall be kept secure at all times.

- **System Key Configuration and Permissions**

  Programming Permissions: System Keys will be issued with restrictions allowing the User to configure a *specific set of subscriber features* per the rights granted to the User by the Key User Agreement. System Keys will typically be locked down to permit modifications to the following:
  - Range of Talkgroup IDs and Radio IDs designated to the programmers' user base
  - The SIRN Mutual Aid Trunked Talkgroup IDs
  - Other talkgroup or SIRN system data per other agreements between programmer and user base

  Time limit: All keys generated by the System Administrator will have an expiration date set. Expiration of System Keys will be set to six months. Users seeking to maintain authorization for System Key access will be required to recertify by completing the certification standards listed in this policy.

- **System Key Administration**

  Each radio vendor's Master System Key will be in the possession of the System Administrator.

  Only the Statewide System Administrator will develop system keys copies for distribution to agency programmers and third party-radio shops. No other agency or service shop may distribute or duplicate

System Keys to other third parties for any reason.

Each key will be provisioned with user-specific permissions.

System keys will be logged and tracked. The System Administrator will track all keys and a corresponding list of authorized agencies and individuals with access to System Keys.

System Administrator may conduct routine audits of persons responsible for the keys.

The SIEC reserves the right to amend this policy at their sole discretion in order to increase the security and protect the integrity of the system. SIEC reserves the right to revoke the ability to possess a key if the agency's possession affects the integrity and/or security of SIRN.

5. Recommended Procedure

- **System Key Authorization and Issuance Process**

All agency or third-party personnel seeking permission to use SIRN System Keys shall obtain authorization by completing and submitting the *Programming Keys Request/Authorization* to the SIRN Statewide System Administrator.

System Keys Users will only be issued to:

- State or local North Dakota agency personnel responsible for self-maintaining agency devices
- Commercial service shops under contract for subscriber programming and maintenance by an approved SIRN user agency (vendor agreement between the programmer and user agency may be required as evidence)

Standards for Certification as a System Key User: All personnel—self-maintained agency and commercial service shop—requesting access to System Keys shall:

- Complete a background check per the State of North Dakota Information Technology (NDIT) guidelines
- Complete the programming training course applicable to the device and be certified for use of the radio manufacturers' radio programming software and hardware tools.
- Certify knowledge of the SIRN programming and interoperable communications/fleetmap standards, and attend any required SIRN radio programming webinars

Prior to approval, the SIRN Administrator may also elect to interview System Key requestors to validate their experience in radio programming and codeplug development.

System Keys for non-Motorola devices shall, in principle, follow the same standards described above. Agencies or individuals seeking to obtain SIRN System Keys must:

- Meet the standards for certification as a System Key User
- Complete the *Programming Keys Request/Authorization* for submission to the SIRN

Network Manager.

On behalf of the requesting agency, the SIRN Statewide Administrator will make the request for the System Key to the manufacturer and obtain the Master System Key *directly*. The Administrator may then elect to:

- Issue clones to System Key Users, or
- Authorize the third party manufacturer to issue cloned System Keys directly to the requesting agency or individual.

System Key Users accept full responsibility for the use of the keys and will adhere to this Policy.

Approved System Key Users may only use the keys to program radios approved for SIRN access. It is the responsibility of the System Key User to validate, through the SIRN Administrator, an executed agreement, or other official documentation (notably database listing SIRN Contracted Vendors and their respective customer agencies), that their customer is an authorized SIRN User prior to using their issued System Key to program that user's device.

All System Key Users shall:

- maintain current and accurate records of all radio programming performed, including codeplug development/modification activities, and
- provide *quarterly reports* to the SIRN Administrator of all radios programmed.

A System Key User found to be responsible for a SIRN breach due to non-compliance with the policies herein will void their System Key User privileges and, in addition, be responsible for the cost of mitigation activities necessary to resolve the breach.

- **Liability for the Misuse of the System Keys**

Each agency or third-party radio services vendor must designate a primary and an alternate employee ("System Key Users") who will be responsible for obtaining and security of the system key(s) within the organization. Each employee with access to System Keys shall go through the certification process in this policy. While not mandated, entities are encouraged to create their own internal policy to ensure compliance. System Key User agree to the following:

1. System Key Users absolve SIEC and SIRN representatives of all liability involving the loss or misuse of the system key(s) they signed for and took possession of for their agency.

2. System Key Users will be personally and professionally liable for the misuse and/or loss of system keys while in their possession. The agency representative will not be liable for the loss or misuse of a system key while in the possession of the agency alternate or vice versus unless the agency user's policy assigns such liability. If this is the case, the SIEC will follow the most stringent policy in determining liability and the ability for individual users to have future access to the system.

3. If the misuse and/or loss of a system key is discovered by the agency representative and/or agency alternate, then the violation must be reported *immediately* in writing to the SIRN Statewide System Administrator. SIEC stresses the importance of reporting the misuse or loss of a system key, as a failure to report could result in the loss of the key or access to SIRN by the agency. To protect the integrity and security of the system, access to the system keys will be immediately suspended until the issue is resolved. Please review SIRN Standard 7.2.0 "Response to Non-Compliance" for additional information.

4. The misuse and/or loss of a system key could result in the agency representative's and agency alternate's access to SIRN being permanently revoked.

6. Management

Assumptions: SIEC assumes there will be individuals qualified to serve as the SIRN System Administrator and the System Administrator's Designee, and these individuals will be able to successfully carry out their required duties.

Liabilities: The manner in which the standard is drafted keeps a majority of the liability with the individual agency users and the individuals employed by SIRN to carry out the required duties and apply to the extent recognized by North Dakota Code.

Cost: The cost of this Standard is unknown. Some costs could include filling the position of SIRN System Administrator and System Administrator Designee (search, background checks, possible salary, etc.).