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

Document Section	**2 – Management of System**	**Status**: SIEC Sub Committee Approval Date: 1/31/2022
State Standard Number	**2.11.0**	
Standard Title	**System Management Login Accounts**	
Date Established	**1/25/2021**	**SIEC Approval**:
Replaces Document Dated	**NA**	
Date Revised/Reviewed	**1/31/2022**	1/31/2022

1. Purpose or Objective

The objective of this standard is to provide a procedure for managing ***Core Support Users'*** Login Accounts. Core Support Users include SIRN system administrators, technical support staff and managers.

2. Technical Background

- **Capabilities**

SIRN employs multiple applications and databases, collectively referred to as Network Management Systems (NMS), to monitor, configure, maintain and manage all the network core and system devices. Access to these Core Services is enabled via regulated Login Accounts.

Login Accounts are assigned to individuals. One Core Support User may be assigned multiple accounts based on their access rights as determined by technical and security experts and as approved by the Statewide System Administrator.

Any staff logging onto the system to use the applications and support tools are referred to as "Login Users". Login Users include System Managers, System Administrators, and Technical Support Staff.

- **Constraints**

Every user login ID must be unique to simplify managing user accounts. Login user IDs will be unique, will not be duplicated anywhere in the system and will be provisioned only for the services, applications and functions the Login User is approved.

3. Operational Context

SIRN network management applications provide Login Users the ability to manage, configure, provision, monitor and maintain virtually all network resources, system devices and end users. Given the broad and vital capabilities of Login Accounts, access to the network management applications will be closely controlled and managed by the Statewide System Administrator.

4. Recommended Protocol/ Standard

The Core Support Users Login Accounts will be managed by the Statewide System Administrator. Login Accounts issued to individuals will be configured to access *only the system functions and resources* for

which the Login User is responsible and has the required training credentials. See SIRN *Standard 2.17.0 Technical Staff and Maintenance Providers Training and Qualifications* for additional details on training requirements and qualifications.

This Standard also applies to the creation and management of Provisioning Manager (PM) security groups and accounts used to configure and administer user resources such as talkgroups, radios and consoles. Login Accounts for PM security groups will be organized and assigned by the Statewide System Administrator as required.

5. Recommended Procedure

Only the Statewide System Administrator shall issue or provision Core Support User Login Accounts.

Sole Use:

- Login Accounts are for sole use. Users are NOT permitted to share their Login Accounts with any other individuals within or outside of their agency. Each individual requiring and approved for access shall have a distinct Login Account.

Unique ID: User IDs will be developed using guidelines established by technical experts to ensure all user IDs follow a standard format and no user ID is duplicated.

Read Only Access: Depending on access privileges, some Login Accounts may be configured for read only access allowing the user to read and review network settings and user provisioning data, without privileges to make changes.

6. Management

The North Dakota State Interoperable Executive Committee (SIEC) is responsible for updating this procedure.

Assumptions: The Standards Working Group assumes the SIEC and technical experts will strictly adhere to the Standard.