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	**2.18.0**	
Standard Title	**System and IT Network Security**	
Date Established		**SIEC Approval**:
Replaces Document Dated	**NA**	
Date Revised/Reviewed	**1/31/2022**	1/31/2022

1. Purpose or Objective

The purpose of this standard is to establish policy and procedure on IT and system security requirements for preserving the security and integrity of the SIRN's core network services through proactive monitoring/detection, security and anti-virus upgrade plans, proper network firewall designs, diligent user/operator authentication, and training.

2. Technical Background

Capabilities
SIRN is a complex set of operating systems, software and hardware assembled from a multitude of third-party Commercial-Off-The-Shelf (COTS) providers. A comprehensive IT security plan covering all systems, subsystem and individual hardware/software has the overall benefit of protecting the functionality, integrity, and operation of the system.

In addition, SIRN does not exist in a vacuum—it is connected to a variety of IP networks and applications including municipal enterprise systems, CAD applications, fault management systems and others. A comprehensive anti-virus plan, well-conceived firewalls regulating network ingress/egress, and real-time monitoring are all essential for the system's security posture.

Constraints
IT systems are subject to intentional attack or can be unintentionally compromised, both of which can have wide implications on the performance of SIRN.

3. Operational Context

Technical security plans coupled with user training of potential IT security risks are essential to preserve system integrity.

4. Recommended Protocol/ Standard

SIRN shall have the following levels and approaches to enhancing security:

- *Real Time Monitoring and Notification*:
    - Network Operations Center (NOC) monitoring of system health and detection of security

breaches
    - Monitoring of site access alarms and maintaining site access logs
    - Prompt notification of service providers and technical staff when system issues occur
    - Prompt notification of affected or compromised users
- *System Access Security and Management*:
    - Coordinated user, operator and maintenance provider authentication and login/password management. All applications and maintenance terminals must be accessed only through password-protected user login accounts.
    - Use of secure methods such as SSH and VPNs to access the Core Network and all other remote elements.
- *Encryption*:
    - Encryption of data while in storage and in transit where applicable
- *Back Up and Recovery*:
    - Routine backup and recovery protocols for system configuration and user databases.
- *Perimeter Security*:
    - Use of Demilitarized Zones (DMZs) and firewall isolation between all SIRN and other ancillary enterprise and data networks (e.g., carrier backhaul, CAD applications, etc.).
    - Approval of any and all external device connections (computers, modems, routers, hard drives, etc.) by the Statewide System Administrator.
- *Physical Security and Staff Credentialing*:
    - Physical access to facilities hosting the Network Core or remote RF sites must be closely controlled; only approved staff with authorized access can access facilities.
    - The Statewide System Administrator shall maintain and update a list of all state and local service providers and their access credentials. Notifications of urgent staff issues, such as discharged employees or cancelled vendor contracts, will be immediately forwarded to all Administrators.
    - Unauthorized staff at equipment locations will be under the direct supervision of authorized staff at all times.
- *Proper User and Technician Training*: Training of technical and operations personnel accessing SIRN, including Administrators, PSAP dispatchers and vendor/in-house technicians.

5. Recommended Procedure

The SIRN Administrator is responsible for:

- Overseeing the implementation of routine security and anti-virus updates
- Evaluating historical security logs provided by the NOC

- Managing user and operator login and access information

All Administrators and technical staff are required to undergo Security Training regularly to maintain access rights to SIRN.

6. Management

SIRN Statewide System Administrator is responsible for managing this Standard.