Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Security Equipment Sites**		Date Created:		12/20/2018	
Standard Policy #	**2.14.0**	Section Title:	**Management of System**		Status	Completed
Approval Authority:	**ISICSB**		Adopted:	**2/14/2019**	Reviewed:	**2/14/2019**

1. Purpose or Objective

The purpose of this standard is to define specific security measures for system and subsystem equipment and to define site security policy.

2. Technical Background

- **Capabilities**

Security measures have the overall benefit of protecting the functionality, integrity, and operation of the system.

- **Constraints**

Details of specific security measures cannot be included in a public standard without compromising security of the system.

3. Operational Context

Equipment and site security is an ongoing process.

4. Recommended Protocol/ Standard

Technical system information which could compromise system security is considered non-public, as defined in various other standards. This information is not to be released to personnel who do not have a legitimate need to know.

Equipment "owned" by a specific agency shall not be altered by another agency without the owning agency's knowledge and consent, as defined in the Maintenance standards for the system.

The system network is to be protected from other data networks by isolation or by using a properly configured firewall having the approval of the Statewide System Administrator.

Any remote access points to the system will be kept secure, with coordination through the Statewide System Administrator.

Equipment owners will password protect their respective system equipment, where applicable, for the purpose of preventing unauthorized access.

User login accounts will be password protected at an appropriate level of protection. If a password is suspected of being compromised, it will be immediately updated to a new password.

External devices (computers, modems, routers, etc.) shall not be connected to the system network without the approval of the Statewide System Administrator.

Site access lists will be kept up-to-date, including vendor support staff. Any person not identified on the list for a site will be denied unsupervised access to that site.

Unauthorized staff at equipment locations will be under the direct supervision of authorized staff at all times.

Notifications of urgent staff issues, such as discharged employees or cancelled vendor contracts, will be immediately forwarded to the other respective owners of the system.

Specifics for monitoring site access alarms are at the respective site owning agency's discretion. Site access shall not be unreasonably denied to agency support staff responsible for maintaining equipment located at that site.

System access shall not be unreasonably denied to agency support staff that would interfere with their system maintenance responsibilities.

Solely owned sites shall be managed by the owning agency Subsystem Administrator. Co-located or shared sites are the responsibility of the entity that allows or grants access.

5. Recommended Procedure

Specifics of procedures not defined within the System Management or Maintenance standards are the responsibility of the Statewide System Administrator.

System manuals pertaining to security are classified as "Security Information" and "General Non- Public Data," pursuant to Iowa Code 22.7(50).

6. Management

Entities that own system or subsystem equipment or entities with interconnected dispatch centers are responsible for the equipment and site security for their respective portion of the system.