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

ISICS Standard: Equipment Site Security	**Standard #:**	2.14.0
	Date Adopted:	02/14/2019
	Date Reviewed:	4/11/2024
	Version:	2.0

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.

The system network is to be protected from other data networks by isolation or by using a properly configured firewall approved by the ISICS System Administrator.

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

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

Unauthorized staff are only permitted at equipment locations when under the constant direct supervision of authorized staff.

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.

Site access alarms monitoring procedures are at the respective site owner agency's discretion. Site access shall not be unreasonably denied to agency support staff with site 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

Specific procedures not defined within the System Management or Maintenance standards are the responsibility of the ISICS 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.