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

ISICS Standard:	**Standard #:**	7.1.0
Standards Compliance ~~Process~~Evaluation / Non-Compliance Procedures	Date Adopted:	08/09/2018
	Date Reviewed:	
	Version:	

1. Purpose or Objective

The purpose of this S~~s~~tandard is to describe the process by which users of ISICS will be evaluated to ensure compliance with the standards, policies, and procedures set forth by the Iowa Statewide Interoperable Communications System Board (ISICSB)~~,~~ and to detail the procedures and actions for non-compliance as set forth by the ISICSB. ~~Evaluations may be scheduled and/or non-scheduled.~~

2. Technical Background

- **Capabilities**

  N/A

- **Constraints**

  N/A

3. Operational Context

The ISICSB is charged with setting standards and determining protocols and procedures for the most efficient and effective operations between and among users of the ISICS platform.

The improper use of ISICS Platform resources can have minor to grave consequences. These standards, policies, and procedures have been set forth by teams consisting of radio users and managers to maximize service and to minimize potential negative consequences. Responsible management of this resource requires that compliance be evaluated.

4. Recommended Protocol/Standard

DRAFT

Scope

This procedure applies to all users and stakeholders of the ISICS platform.

The ISICSB Chair, System Administrator, the Operations Committee, ~~and~~ the Technical Committee chair~~s~~, or Sub-System Administrators, may call for an evaluation of user compliance in response to an event or incident that caused an outage or damage to or had the potential to cause an outage or damage to users or resources of the ISICS Platform. Events and incidents may include evaluating outcomes that consistently show non-compliance.

Consequences of failure to comply with these standards, protocols, and procedures fall into three categories of non-compliance:

- **Imminent threat**
- **Major Damage or Disruption to the System**
- **Minor Consequences to the System**

Imminent threat due to Non-Compliance

1. If an imminent threat is perceived to affect the system that cannot wait for formal action by a committee, the System Administrator is empowered to take immediate, corrective action at their discretion, and the below ISICSB members and stakeholder(s) will be notified:
    - ISICSB Chair
    - ISICSB Vice Chair
    - The appropriate Subsystem Administrator(s)

    This includes but is not limited to denial-of-service attempts by rogue radios, technical malfunction of subscriber units that may make the system unavailable for other users, or other issues that may negatively affect system access by other users.

    If a user suspects an imminent threat exists, they should immediately call their Subsystem Administrator. The Subsystem Administrator will notify the System Administrator of the incident if they determine that is necessary.

Major Damage or Disruption to System due to Non-Compliance

1. **Incident Identification**
    - Any user or stakeholder can report an incident or event that potentially disrupts or damages ISICS Platform resources.
    - Reports should be documented with details including date, time, nature of the incident, and involved parties and presented to ISICSB Chair, ISICS System Administrators, or the SWIC.
    - Notifications can be made at ISICSNOC@dps.state.ia.us or 515-725-6095
2. **Initial Assessment**
    - Upon receipt of a report, the System Administrators or designated authority will conduct an initial assessment to determine the severity of the incident.

Formatted: Font: Not Bold, No underline

Formatted: Normal (Web)

DRAFT

- Evaluate whether the incident resulted in an outage, damage, or poses a significant risk to users or resources.

3. **Evaluation Call**
   - If the initial assessment indicates significant impact, the System Administrator will determine the need for a formal evaluation.
   - The evaluation call can be initiated in response to:
     - Direct incidents.
     - Patterns of non-compliance observed in system usage reports.
4. **Formation of Evaluation Committee**
   - A temporary evaluation committee will be established, including:
     - Chairperson (ISICSB Chair or designee)
     - Relevant system administrators
     - Members from the Operations and Technical Committees
     - SWIC and additional experts as necessary
5. **Data Collection**
   - The evaluation committee will collect and review all relevant data, including:
     - Incident reports
     - System logs
     - User compliance records
     - Any additional documentation pertinent to the incident
6. **Analysis**
   - Conduct a thorough analysis of the collected data to determine:
     - The root cause of the incident
     - Patterns of non-compliance
     - Impacts on system functionality and user operations
7. **Recommendations**
   - Based on the analysis, the evaluation committee will draft recommendations to:
     - Address the immediate issue (e.g., remedial actions, resource adjustments).
     - Prevent recurrence (e.g., updated protocols, training sessions, system updates).
     - Improve overall compliance and usage standards.
8. **Implementation of Recommendations**
   - Following approval from the ISICSB, the responsible parties will implement the recommended actions.
   - Timelines and responsibilities for each action item should be clearly defined.
9. **Monitoring and Follow-Up**
   - Continuous monitoring of compliance will be instituted to evaluate the effectiveness of implemented recommendations.

Minor Consequences due to Non-Compliance

1. **Non-compliance Identification**

DRAFT

- Any user or stakeholder can report an incident or event that potentially disrupts resources or causes minor infractions related to ISICS platform usage.
- Reports should include details such as the date, time, nature of the non-compliance and the involved user(s).
- Notifications can be made at ISICSNOC@dps.state.ia.us or 515-725-6095

2. **Initial Review**
   - The ISICS System Administrator or designated authority will review reported deviation from written standards.
   - This may include improper usage of resources, failure to follow protocols, or non-compliance with established standards that do not pose immediate risk.
3. **User Notification**
   - The SWIC, System Administrator, ISICSB Chair or designee will then notify the user(s) involved in the non-compliance via email or direct communication, summarizing:
     - The nature of the reported issue.
     - Relevant policies or standards that were not followed.
     - The potential impact of such non-compliance of standard on the system and other users.
4. **Opportunity for Response**
   - Allow the user(s) to provide context or explanation regarding the non-compliance of standard or procedure.
5. **Evaluation of User Response**
   - Review the user's response to determine if further action is warranted.
   - If the response provides valid context or demonstrates a commitment to compliance, it may be considered in the next steps.
6. **Corrective Action**
   - Based on the evaluation, determine appropriate corrective actions, which may include:
     - Additional training or resources to reinforce compliance.
     - A short-term monitoring period to ensure adherence to protocols.
7. **Communication of Actions Taken**
   - Communicate the outcome of the review and any corrective actions to the user(s) involved.
8. **Reporting to Committees**
   - Summarize this procedure and actions taken in regular reports to the Operations and Technical Committees.
   - Use these insights to refine policies and procedures continuously.

5. Recommended Procedure

Non-compliance may come to the attention of various personnel as a result of routine monitoring, an audit, a report, complaint from radio users, or other sources. Any individual discovering non-compliance will immediately report it to their Local System Manager or

DRAFT

Subsystem Administrator. If the issue cannot be resolved at the local level, the Statewide System Administrator will notify the Governance Committee Chair and the ISICSB Chair of non-compliance.

The Subsystem Administrator or Statewide System Administrator will follow up to ensure that all next steps and/or corrective action has been completed within the time frame established by the ISICSB.

Conclusion

Adherence to this procedure will foster a culture of compliance, enhance the reliability of the ISICS platform, and mitigate risks associated with improper use of resources. By systematically evaluating incidents and encouraging responsible management, we can ensure the platform serves its users effectively and efficiently.

~~The results of the evaluation will be forwarded to the Standards Committee for review and possible counsel with the Governance Committee to determine which ISICS standard(s) the agency was in non-compliance.~~

~~The findings of this review will be forwarded to the ISICSB. With the available findings and evidence, the ISICSB shall review the case with appropriate entities and decide on an appropriate course of action for non-compliance.~~

6. Management

The ISICSB Chair, acting on behalf of the Iowa Statewide Interoperable Communications System Board, will manage this process.

DRAFT