Integrated Public Safety Commission

100 N. Senate Ave., N825 Indianapolis, IN 46204

Integrated Public Safety Commission (IPSC)
Encryption Policy

Policy Adoption/Effective Date:	December 12, 2023
Policy Approved By:	Integrated Public Safety Commission (IPSC)
Policy Last Updated:	December 12, 2023

BACKGROUND:

The Integrated Public Safety Commission (IPSC) has been statutorily charged with the responsibility of providing voice and data interoperable for public safety communications in Indiana.

Numerous public safety agencies and governmental disciplines use 700/800 MHz trunked and conventional radios intended to provide interoperable communications between all public safety and governmental disciplines.

PURPOSE:

The purpose of this policy is to ensure the safety, security, and interoperability of participating public safety agencies regarding the programming, key loading and use of encryption features on 700/800 MHz SAFE-T radio system.

POLICY:

To ensure the safety, security, and interoperability of the SAFE-T LMR radio system, IPSC has adopted the following measures related to encryption on the SAFE-T system:

1. As of the adoption date of this policy – IPSC will no longer support the Data Encryption Standard (DES), 56-bit encryption, as it is far less secure than the recommended Advanced Encryption Standard (AES) 256-bit algorithm.
    a. In 2005, the National Institutes of Standards and Technology (NIST) withdrew its approval of DES as a federal encryption standard
    b. Federal Information Processing Standard 140-2 (FIPS 140-2) requires all federal agencies to use AES encryption
    c. As mandated by the Cybersecurity Enhancement Act of 2014, any state or local agency wishing to interoperate on a federal LMR system must also have AES encryption on their subscriber units.
2. As of the adoption date of this policy – In order to ensure interoperability coordination, any new talkgroups created after said date on the SAFE-T system will be configured to operate "in the clear" only.
    a. This means that encryption will not be possible on the talkgroup, unless coordinated and activated by the IPSC Integrated Connection Center.
    b. To do so, please contact the ICC at icc@ipsc.gov or (317) 234-1450

3. As of the adoption date of this policy – All wireline console users must coordinate encryption settings through IPSC. Settings must be entered into Provisioning Manager in a manner that does not conflict with existing encryption in use by other agencies.
    a. All Storage Location Numbers, or SLN, must be reserved through the IPSC Connection Center to avoid duplication.
    b. The Patch Key in each console must match IPSC's currently in-use key so interoperability is not compromised.

DEFINITIONS:

- Encryption – Digital radio encryption is the process of using an algorithm to encode information (voice or data) that is unable to be accessed by anyone without the proper key.
- Advanced Encryption Standard (AES) – 256 bit algorithm, recommended as the best practice for use on the IPSC system, as well as recommended by the National Institutes of Standards and Technology (NIST) and Cybersecurity and Infrastructure Services Agency (CISA).
- Digital Encryption Standard (DES) – 56 bit algorithm, not recommended for use by IPSC/NIST/CISA.

REVISION HISTORY:

Date:	Responsible Party:	Change Summary:
December 12, 2023	Integrated Public Safety Commission (IPSC)	Initial Draft Approved by Commission