Statement of Understanding and Acknowledgement

The Consolidated Communications Network or Colorado, Inc. (CCNC) in collaboration and cooperation with the State of Colorado Public Safety Communications Network (PSCN) team recently adopted a policy addressing the public safety Digital Trunked Radio System (DTRS) network security issues. The newly adopted policy is contained within the CCNC Policy and Procedures (P&P) Manual. The entire manual may be viewed at www.ccncinc.org under the Applications and User Documents. The newly revised and adopted Chapter 10 of the P&P may be located in the manual under CCNC POLICY & PROCEDURES; Chapter 10 MEMBER RIGHTS AND RESPONSIBILITIES; Section 10.7 – MONTHLY WINDOWS RESTART OF ATTACHED WORKSTATIONS AND ASSOCIATED HARDWARE.

This policy explains the critical mandate to restart all devices connected to the DTRS network monthly in order to keep the DTRS as secure and protected from cyber security incursions as is possible. The policy defines sanctions that must be taken in order to ensure compliance with the policy. A single connected network device that is not restarted in order to take the monthly security updates poses a risk to the entire DTRS network for all DTRS users, including all first responders using the DTRS.

Please read very carefully the attached policy. It is important that you fully understand the policy, the sanctions imposed as a result of non-compliance, and that you acknowledge your understanding and agreement to strictly adhere to the policy.

Acknowledgement:

The undersigned hereby acknowledges that they have read the attached revision to the CCNC Policies and Procedures; Chapter 10; Section 10.7 regarding Monthly Windows Restart of Attached Workstations and Associated Hardware.

I understand that I can contact any CCNC Executive Board Member or Regional Director if there is any aspect of this policy that I do not understand or about which I wish to see further clarification.

I understand that failure to comply with any provision of this Policy may result in corrective action and firm sanctions.

Signature – Title Date

Printed Name –Title

Consolidated Communications Network of Colorado, Inc. (CCNC) Policies and Procedures

Chapter 10 – Section 10.7

10.7 MONTHLY WINDOWS RESTART OF ATTACHED WORKSTATIONS AND ASSOCIATED HARDWARE

10.7.1 Definitions:

Connected devices are defined as:

Console equipment: Workstations commonly referred to as consoles which include a windows central processing unit (CPU), monitor, voice processing module (VPM) and may include speakers, footswitch, microphone, headset, and other accessories.

Logging recorder devices: Are computer devices provided through local purchase from various vendors for the purpose of digital recording of radio traffic, such recordings often stored and used as evidence or historical reference.

AIS: Archiving Interface Server workstations, commonly referred to as an AIS, are used to interconnect logging recorders, Computer aided dispatch (CAD) or other applications to the radio network.

CAM Server: Console Alias Manager (CAM) is a Windows workstation that allows for local management of Unit IDs and Aliases.

Console Proxy Server: An Application that converts audio packets inside the radio network to be sent outside the radio network to an MCC 7500E Dispatch console.

NM Clients: Network Management Clients (NM Clients) consist of a windows workstation with Motorola software that allows the user to perform functions and request information based upon selected permissions associated with that users login credentials.

First half of the month: Is the 1st day of every month through the 15th day of every month.

Second half of the month: Is the 16th day of every month through the last day of every month.

DTRS: Digital Trunked Radio System. For the purpose of this document we are referring to all the zones and sites interconnected to make up the Statewide Colorado public safety radio system owned by the State of Colorado and local governmental infrastructure owners.

PSCN: Public Safety Communication Network. The designated state division responsible for oversight operations and the installation, operation, and maintenance of the DTRS equipment.

10.7.2 Description:

Due to the potential risk and related severity of a breach of security of the Public Safety Radio infrastructure, it is mandatory that the most current "MOTO Patches" be pushed out through the network by the DTR System Engineers on a monthly basis, between the first day of every month and through the fifteenth day of every month. In order for all of the above defined hardware attached to the DTR System, such as workstations, logging recorder devices, console equipment, AIS and other windows operating subsystems be in a ready state to accept, install and implement the monthly patches, all defined devices shall be restarted monthly between the 16th day of every month and the last day of every month. The restart of the Windows operating system, not just the Motorola applications, shall be accomplished by closing applications and then choosing the 'Restart' option from the power options on the menu.

If a breach of network security caused by a malicious virus, mal-ware, trojan, bot, or any other network security breach is traced to a device not in compliance with this Section 10.7, the device will be immediately disabled from the system and all costs related to any interruption in delivery of public safety communications to any CCNC member agency, all damages, and full costs of recovery of the public safety communications network will be borne by the violating agency.

The following steps and procedures are instituted for agency users who fail or repeatedly fail to restart the appropriate hardware between the 16th day of every month and the last day of every month, posing a threat and risk to the public safety communications system. Posting any known vulnerability on a public facing website is prohibited.

10.7.3 First Offense:

Defined as failure to restart each and every connected device between the 16th day and the last day of every month. Any device listed as not ready to accept and install the monthly patch to the DTR System Engineer pushing out the Motorola patches will be force restarted without prior notification to the agency. There is no assurance that the device will restart normally following the forced restart, and there is no liability should the device fail to restart. There will be an effort to avoid disabling an entire dispatch center. The DTR System Engineer providing the Monthly System Report during the CCNC Technical/Operations meeting will provide a list of the violating agencies not restarting during the previous 30-day period. The CCNC Regional Executive Board member for each region will receive a list of violating agencies within their region from the Administrative Assistant. The CCNC Regional Directors will make contact with each agency or department failing to comply with this policy. The Regional Directors will discuss this policy and agency responsibilities to comply with the restarting policy. Once the agency informs the Regional Director of their changed method of meeting compliance by restarting the associated devices, the Regional Director will notify the DTR System Engineer that the violating agency has been notified and offered evidence of internal policy to achieve and maintain compliance.

10.7.4 Second Offense:

Defined as failure to restart each and every connected device between the 16th day and the last day of every month, regardless if a consecutive or recurring monthly violation, further defined as a second violation within a 12-month period. The second offense will be handled in the same manner as the first offense for forced restarting, reported to the CCNC by the DTR System Engineer providing the Monthly System Report at the CCNC Technical/Operations meeting. The violating agency head (Sheriff, Police Chief, Fire Chief, Mayor, 9-1-1 Authority, Comm Board, etc.) will receive a letter from the CCNC

President requiring a two-week written response detailing the process and steps the agency will institute to ensure their hardware does not become a three-time violator. The letter will recommend they discuss any questions they have with any of the CCNC Regional Directors or the DTR System Engineer. The agency head will be required to notify the appropriate Executive Board Regional Director when the corrective actions have been implemented. The DTR System Engineer will be notified by the Regional Director when the agency has provided the appropriate notice of corrective action. The letter will include a reminder of the consequences for a third violation.

10.7.5 Third Offense:

Defined as failure to restart each and every connected device between the 16th day and the last day of every month, regardless if a consecutive or recurring monthly violation, further defined as a third offense within a 12-month period. In order to protect the integrity of the public safety communications network, the device or devices will be force restarted by the DTR System Engineer. The third violation will be reported to the CCNC Officers by the DTR System Engineer. It shall be the responsibility of the CCNC Officers and/or Regional Directors to make reasonable attempts via all methods of contact available to contact the violating agency department head or command level staff. The agency director, department head or command level staff will be required to attend, either in person or virtually, a meeting with the CCNC Executive Board and the DTR System Engineer, arranged by the CCNC. The meeting shall address the nature of risk and threat to the public safety communications network and the severity of the agency lack of response to the network security policies. The meeting may include discussion surrounding the agency's desire, or lack thereof, to remain fully committed as an integrated agency with connectivity to the network core. The agency will be granted a period of five business days to provide documentation defining local policy and procedures for restarting all devices connected to the DTR System. Upon receipt of the agency policy and procedures, the CCNC Executive Board and the DTRS Engineer shall review for document approval and acceptance. A follow up meeting may be requested with the agency director, department head or command level staff to assess the successful implementation of the local policy and compliance with this CCNC policy.

Agency failure to acknowledge and comply with the conditions of this Section 10.7.5 may result in extreme sanctions. Those sanctions may include assessed fees related to cost recovery. Cost recovery fees will be calculated on an escalating scale and will be applied to each device not in compliance and per violation. Repetitive violations may result in disabling the network port, thereby disconnecting the device from the network.

10.7.6 Reoccurrences of Offenses:

The offenses of failing to restart attached workstations is intended to be in a 12-month period, not a calendar year. The timeframe for any agency begins with the first offense. Example: If your agency fails to restart your NM Client in January 2022, your 12-month period concludes at the end of December 2022.

10.7.7 Disconnected Equipment:

If any windows workstation is temporarily disconnected from the DTR System by the device owner for any length of time, causing it to miss one or more monthly MOTO patch software update(s), the DTR System Engineer must be notified of the intent to reconnect the equipment. The DTR System Engineer will coordinate with that agency to ensure that the equipment is downloaded with all current software updates and MOTO Patches prior to reconnection in order to protect the network from security breaches.