COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM

SYSTEM KEY APPLICATION AND AGREEMENT

Application Date: _____

Applicant Name: _____

Applicant Email: _____

❑EFJohnson ❑Harris

❑Kenwood ❑Motorola

❑Tait Other_____

Applicant Agency / Company Name:_____

Mailing Address:_____

City:_____ State:_____ Zip Code:_____

Agency / Company Point of Contact:_____

POC Telephone Number:_____

POC Email Address:_____

Anticipated Date of Implementation:_____

Agency / Company Type: Agency Self Maintained ☐ Private Service Provider ☐

Agency MAC Region: Metro ☐ Northeast ☐ Southeast ☐ Southwest ☐ Northwest ☐

Primary DTRS Zone Controller used (if known):_____

Training Provided By (Name / Agency):_____

Signature:_____

Date Training Completed:_____

If Training is not completed, provide scheduled date and trainer information:

_____

_____

Has the applicant ever had a System Key(s) issued by the State of Colorado or CCNC? Yes☐ No☐

Has the applicant ever had a System Key(s) revoked by the State of Colorado or CCNC? Yes☐ No☐

Briefly explain level of programming needed and who you will be programming radios for: (i.e. local agency only need; provide programming for County level entities; provide for Zone level programming; provide regional level programming; provide service provider level programming):_____

_____

_____

_____

_____

_____

_____

_____

_____

**********ADMINISTRATIVE USE**********

BACKGROUND: ❑Fingerprint Card ❑Agency Letter Sent to CBI:_____ Returned:_____

TRAINING: ❑Proof Provided

CCNC EXECUTIVE BOARD: ❑Approved ❑Denied Date:_____

INVOICE: Date sent to Applicant:_____ Date Payment Remitted:_____

DATE KEY PROVIDED:_____

SYSTEM KEY AGREEMENT AND POLICY STATEMENT

Participating agencies in the Colorado Statewide Digital Trunked Radio (DTR) System and CCNC have operational needs that require the use of various talk groups to meet their communication needs.

Agencies need to be able to manage the use of their agency talk groups to meet their agency communications requirements and expectations. Agencies may also have need for communications with other CCNC users or with radio users from other systems outside of the DTR. Agencies must be able to satisfy these communications requirements in ways that are both effective and efficient while maintaining the integrity of the system fleet map. Fleetmap information is system sensitive information that should not be divulged without proper security procedures and a valid need to know. The user agency needs must be balanced with the system security and capacity requirements so as not to have an adverse effect upon system performance.

There is no implied or expressed authorization provided by CCNC that grants access to others systems, Zone Controllers or switches through this Application and Agreement. Authorization to program any other system will be separate from this agreement and between the agencies requiring the cross system programming. It is strongly recommended that a reciprocal sharing agreement be completed between the various system key holders. Authorization should be obtained in writing from the designated representative of a connected DTRS Zone Controller and submitted with this application.

The *COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT* submitted to CCNC will be reviewed by the CCNC Executive Board as to the need to grant a system key to the applicant; the Zone Controller owner interest is weighed, and approval or disapproval will be their charge. *The CCNC Executive Board reserves the right to refuse a DTRS System Programming Key to an applicant.*

DEFINITIONS

- Fleetmap
- Radio ID
- System Key
    - Electronic Key
    - Hard Key
    - Soft Key
    - Master Key
    - Subordinate/Distribution Key

FLEETMAP AND RADIO IDS

- The State of Colorado Governor's Office of Information Technology (the State) is responsible for managing the fleetmap information and Radio IDs for all agencies on the system. Some designated agencies and private service providers may maintain a working list of Radio IDs for system addition as needed. Unless otherwise specified, the DTR Monitoring Center is responsible for all new talk groups and Radio IDs to be added to the system. Notification shall be by email to webdtr@state.co.us.
- The system subscriber database is a closed database. Only radios authorized for service on the system are activated in the subscriber database. The State, local government, or their authorized representative(s) are the only personnel authorized to activate and deactivate radios in the subscriber database. When required, notification shall be by email to webdtr@state.co.us.

SYSTEM KEYS

- As the primary System Key Holder the State maintains the Master System Key for all manufacturers of equipment authorized to operate on the DTR. Agencies requesting a system key must complete the *COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT*. The State is responsible for issuing subsequent keys to eligible programming agencies. As secure System Keys become available for various manufacturers equipment they will be issued to programming agencies and the old Software Keys will be destroyed. The use of any DTR System Key and associated equipment is subject to all rules, regulations and policies established by the State of Colorado, CCNC, and the FCC and designated vendor. Any violation will result in the *COLORADO STATE WIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT* being terminated and the DTR System Key revoked.

PROGRAMMING EQUIPMENT

- Each programming agency is responsible for acquiring the proper programming software and equipment necessary to program the radios they support. Each programming agency is also responsible for acquiring their I-button readers or equivalent security hardware if required for programming. When applicable, CCNC will provide the actual I-buttons or equivalent security device to the State for programming with the System Key parameters.
- The System Key remains the property of the State of Colorado. The associated I-buttons or equivalent security hardware purchased by CCNC remains the property of CCNC. Programming software and the required cables purchased by an agency or service provider remain the property of the agency or service provider.
- Any Computer connected to the system or used for any radio programming will have up to date antivirus software installed and maintained.

ELECTRONIC SYSTEM KEY POLICIES

- Agencies requesting a system key will complete the *COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT*.
- System Keys will only be issued, after completion of training, to authorized CCNC members that are self-maintained and use the System for functionality, or to Manufacturer Authorized Service Shops that are maintaining equipment for CCNC Agencies. Approved training is defined as completion of a training course provided by a CCNC approved trainer. Vendor provided courses are encouraged but are not a substitute for the CCNC training.
- No CCNC member agency or designated Manufactured Authorized Service Shop will directly or indirectly permit any third party to: view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with, or otherwise compromise the security of any radio code plug programming file, system key file, encryption key file, or template information for any radio on the system. The System Key will not be distributed or any DTR radio ID's or talk group(s) information disclosed to a third party for any reason. However, DTR System Key holders (except for "write only" system keys) may create code plugs and provide the code plugs to qualified agencies or service providers for programming into subscribers units.
- In the event that a CCNC member agency or designated Manufactured Authorized Service Shop learns that any party has improperly or fraudulently obtained radio code plug file information, system key file information, encryption key file information, or template data, that party will immediately notify the CCNC Executive Board of the security breach.
- Any Agency or Service Provider found to be responsible for a security breach as listed above will be responsible for the cost of all reprogramming to include but not limited to system infrastructure and subscriber programming necessary to overcome said breach.

- Any System Key holder believed to be in violation of any of the System Key Policies shall have their System Key authorization temporarily suspended. The CCNC Executive Board shall review relevant facts from all parties involved in the situation for appropriate action to be taken. The determination of the CCNC Executive Board on reinstatement, suspension or revocation is final.
- System Keys that are capable of expiring will be set to expire as determined by the CCNC Executive Board (generally annually) and will be reissued after re-verification of agency needs. Keys which are issued with 'Write Only' privileges may be set to expire after three years.
- Only ID(s) and talk groups that have received prior authorization from CCNC may be programmed.
- Self-maintained agencies may only program radio ID(s) and talk group(s) of the DTR radio system for their own agency or agencies to which they provide DTR subscriber maintenance. All agencies shall maintain copies of all talk group authorization letters, which are subject to verification by CCNC at any time.
- Private service System Key holders may only program radio ID(s) and talk group(s) on behalf of agencies authorized to use the DTR radio system for which they provide DTR support. Providers shall maintain copies of all talk group authorization letters, which are subject to verification by CCNC at any time.
- All radios will be programmed for write protect file access if the equipment supports the write protect function.
- All radios will be programmed to allow Radio Inhibit from the System Management Terminal.
- Any radio sent to the vendor for repair may be sent with the programming intact. Whenever possible, the sending agency should archive the file from the radio prior to shipping. When radios are returned from Vendor repair, they should be verified.
- All System Key holders shall maintain current and accurate records of all programming performed. Records shall be made available upon request to the State of Colorado or CCNC.

System Security

- All personnel who have access to the DTR system, including sites, site equipment, the system networks, system console equipment and those who have direct responsibility to configure and program subscriber units will be required to pass a state and national fingerprint-based criminal history record check and be granted authorization from the *CCNC EXECUTIVE BOARD*. **For Vendors: If a fee is charged for this background check the cost will be the responsibility of the subject of the background check.**

System Key Application Process and Personnel Background Screening For DTR Systems Access and System Key Access

- Applicant completes System Key application and remits to the State designee. Applicant completes one application per manufacturer key requested.
- If applicant completed a state of residency and national fingerprint-based criminal history check as a condition of employment, the sponsoring agency may provide a letter on agency letterhead, signed by agency executive, indicating the applicant has completed such background check.
- If no letter can be obtained, a state of residency and national fingerprint-based criminal history checks shall be conducted upon assignment for all personnel who have direct responsibility to configure and program subscriber units operating on the DTR system.
- If a felony conviction of any kind exists, the requesting person shall be denied access to the DTR System Key. However, the requesting person or the employing Agency for the requesting person may ask for a

review by the *CCNC EXECUTIVE BOARD* in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

- If the person has an arrest history without conviction for a felony or serious misdemeanor, the *CCNC EXECUTIVE BOARD* shall review the matter to determine if systems key access is appropriate.
- If the person appears to be a fugitive appropriate action will be taken immediately.
- If the *CCNC EXECUTIVE BOARD* determines that DTR system key by the person would not be in the best interest of the CCNC Membership, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
- The applicant shall complete designated manufacturer programming training prior to key being issued. The CCNC Executive Board may approve a system key application contingent on completion of training, at its sole discretion.
- All System Key holders shall annually complete the Colorado Statewide Digital Trunked Radio (DTR) System "System Key Renewal Statement" (Attached) to be signed by system key holders and their employer, certifying that the employee is a current employee and to the best of their knowledge the employee has maintained a clean criminal record.
- If a System Key holder leaves employment it is the responsibility of the employer to notify CCNC, in writing on letterhead, of separation of employment. It is the responsibility of the system key holder to return the key to CCNC within three (3) business days upon separation.
- If a System Key holder leaves employment, and then returns, the key holder shall complete the *COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT*.

Programming Administration Fees

- CCNC reserves the right to set Programming Administration fees for access to System Keys.
- Programming Administration Fees are charged per applicant, per manufacturer, per year. Payment must be remitted to CCNC before any System Key hardware or soft key is provided to an approved applicant.

I hereby acknowledge that I have read, understand and agree to this agreement, all published policies and procedures as they relate to my application for a DTR System Key that are now in place as adopted and published by the Consolidated Communications Network of Colorado. I further acknowledge that the information contained in my application is true and accurate to the best of my knowledge.

Applicant Signatory Printed Name	Title
Signature	Date

APPROVALS:

AGENCY / COMPANY

I hereby authorize the named applicant to make application for a System Key as part of his/her assigned duties.

Authorized Agency / Company Signatory Printed Name	Title
Signature	Date

STATE OF COLORADO

Authorized Signatory Printed Name	Title
Signature	Date

CONSOLIDATED COMMUNICATIONS NETWORK OF COLORADO, INC.

Authorized Signatory Printed Name	Title
Signature	Date

COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM

SYSTEM KEY RENEWAL STATEMENT

I hereby acknowledge that _____, a current employee of _____, and a current System Key holder, has not to best of the company's knowledge been involved in any criminal or other activity that would necessitate the revocation of access to the DTR System or the ability to program subscriber equipment. Both our employee and our company have read, understand and agree to the System Key agreement, all published policies and procedures as they relate to the use of a DTR System Key that are now in place as adopted and published by the Consolidated Communications Network of Colorado. I further acknowledge that this statement is true and accurate to the best of my knowledge.

AGENCY / COMPANY APPROVAL

I hereby authorize the named applicant to continue the use of a System Key as part of his/her assigned duties.

_____ _____

Authorized Agency / Company Signatory Printed Name | Title

_____ _____

Signature | Date

_____ _____

Applicant Signature | Date