Pikes Peak Regional Communications Network

Policy # 02-2002	Adopted:	**Approved by:**

OFFICIAL POLICY: Issuance and Use of System Key by Stakeholder Members

DATE: December 4, 2002

PURPOSE: To authorize the use of the System Key by Stakeholder Members and to provide guidance and requirements for the authorized use and security of the System Key.

SCOPE: This policy applies to all individuals, members, departments, agencies, or vendors authorized to be issued and/or utilize the System Key.

DEFINITIONS:

PPRCN: Pikes Peak Regional Communications Network

Stakeholder members: The agencies of the PPRCN Inter-Governmental Agreement (IGA) that provided funding or equipment for the infrastructure of the PPRCN 800 MHz Trunked Radio System

GENERAL DESCRIPTION: The Stakeholder members are El Paso County, The City of Colorado Springs, and Colorado Springs Utilities. The operational readiness of all radio equipment is paramount to the mission of the Stakeholder members of the PPRCN. The ability to change templates, correct radio identification numbers and to provide properly programmed replacement/spare radios in a cost-effective, expedient and controlled manner is essential to operational readiness of the Stakeholder members. To accomplish this purpose, the Stakeholder members require authorized use of the "System Key". This policy will outline the procedures to procure, secure, document, and utilize the "System Key".

PROCUREMENT OF THE "SYSTEM KEY":

a. The Stakeholder member will submit a written request for a copy of the "System Key" to the PPRCN System Manager. This request will be signed by (1) the IGA signature authority or (2) the appropriate Stakeholder Executive who has the authority to commit the Stakeholder member to an agreement. This request shall also include an outline detailing the following information:

   1) The designated Stakeholder employee with responsibility to sign for, control, and secure the System Key.

   2) The Stakeholders process to meet the two (2) level security requirement outlined in this policy.

3) What departments, agencies, sections the Stakeholder members will support.

4) Each individual who will be an authorized user of the System Key.

b. Any maintenance provider, deemed essential by the PPRCN System Manager to require the System Key, will also meet all of the same requirements as the Stakeholder members.

c. For the purpose of facilitating interoperability, the PPRCN 800 MHz System Key has been provided to an appropriate member of other systems through Inter-Governmental Agreements. A copy of this policy will be provided those agencies so that they will have a written reference to our procedures and understand the seriousness with which we see the need to provide security for the System Key.

d. Upon receipt of the request, the PPRCN System Manager will:

1. Coordinate the request with the Technical Committee to determine if the listed authorized users in the request have the required technical expertise to properly use the System Key. The Technical Committee will act as the PPRCN Board and System Manager's over-site committee on issues in reference to proper use, training, and recommended or allowable feature changes made with the System Key.

2. Prepare a letter with signature blocks of the designated responsible employee and PPRCN System Manager that clearly states what is being signed for, quantity, and references this policy for requirements of security and use. Once signed for, the System Manager will then provide the requested copy of the System Key to the individual.

System Key Security Requirements: Due to the sensitive nature of the System Key, it must be afforded security at all times to ensure that its use does not cause a degradation of service to any authorized user or the loss in accountability of the radios on the system. The System Key is not to be copied by anyone other than the System Manager without the expressed permission of the PPRCN Board. The System Manager must notify the PPRCN Board if he intends to make additional copies. His notification will include whom, and for what purpose, the copies are being made for. The System Key will be maintained on a media (floppy disk or CD ROM) and not copied to the hard drive of a computer so that it can be secured separate from any computer.

Non-Duty Hours: All Stakeholder members, maintenance providers and the System Manager must provide a minimum of two levels of security when the System Key is not under direct supervision or in use. As an example, during non-duty hours the System Key would be in a locked desk drawer, or safe, in a locked office. The authorized individual must maintain the keys to the desk drawer or safe and office. Any additional keys maintained in a key box that requires signature to obtain.

Duty Hours: While in use, the System Key will be considered secured as long as an authorized user is present. The System Key will not be enabled into the programming software or left in a drive of an unattended computer.

Audit: The System Manager, or other designated representative of the PPRCN Board, will be allowed, and assisted by the responsible employee of the stakeholder, to conduct a no notice audit of the security procedures in place, and use of the System Key to insure compliance with this policy. If there are security problems or operational issues that require escorts or technical assistance it will be provided as expediently as possible by the stakeholder. This audit may include insuring that computers surrounding the immediate area of use or where the Key is secured do not have unauthorized copies of the System Key.

Loss or Theft: Theft or loss of the System Key will be reported to the System Manager as soon as possible. The responsible employee of the Stakeholder member agency will initiate an immediate investigation to determine how the System Key was loss or stolen. The System Manager will investigate the procedures to secure the System Key and advise the PPRCN Board of his findings and recommendations.

Documentation: Prior to programming or re-programming a radio a PPRCN Network Change Form (NCR) will be filled out and approved by the System Manager. A Network Change Request detailing all parameters to be changed including radio model, serial number, and ID number will be submitted to the System Manager for approval prior to radio programming. The Network Change Request Form will also be used to change the current template in a radio.

Multiple Radios on One NCR Form: The Network Change Request Form can contain more than one radio if the activity to be completed for each of the radios is the same. As an example, when programming the same template change into multiple radios. When changing duplicate Radio IDs, both radios should be listed on the NCR with an annotation as to which radio you want to have a new Radio ID.

Documenting Template Changes: Programming template changes will be registered on the appropriate form with the System Manager and current operational versions tracked. The System Manager is required to maintain an electronic copy, provided by the Stakeholder member's responsible employee. The System manager will insure current copies of templates be provided to all authorized users of the System Key.

Logging Use of the System Key: The stakeholder member's responsible employee will maintain a log of System Key use that will, at a minimum, serve to validate the date, time, individual, network change request form number, and radios that required use of the System Key. A copy of this log is to be provided the System Manager on the first working day of each quarter.

Use of System Key:

Authorized Use:

Planned: The authorized System Key user will program only those parameters authorized for change by the approved Network Change Request.

Unplanned: Occasionally radio templates or talkgroup layouts require change as radios are moved from one operational department to another or to replace a defective radio with a spare. If the operational situation does not allow time for prior approval by the System Manager, the PPRCN Network Change Request Form will be submitted the next workday and annotated that the change has been completed for operational reasons. This will be the exception and not the norm. Stakeholder members may be required to address this issue with the PPRCN Board if there appears to be a repetitive unplanned use of the System Key.

Unauthorized Use: No Radio ID will be changed or duplicated without the prior approval of the System Manager**.** No new radio equipment will be added to the system without prior approval of the System Manager. Unauthorized use of the System Key will be investigated for loss or theft as described above. Willful negligence or abuse may result in loss of the use of the System Key.

Associated Issues Not Part of the Policy

Restitution

The restitution statement below was a part of the original draft policy. It was taken out of the policy, when presented to the Board, because it became apparent that it needed to be reworded and have legal look at the paragraph and how it applies to the Stakeholder Members.

> **Restitution:** If the PPRCN Board determines that a new system key is required, the Stakeholder member or maintenance vendor found liable will be responsible for all costs of generating a new system key and programming the radios authorized on the network.

SYSTEM KEY ISSUES

The below system key issues statement and process to reach a Positive Subscriber environment statement were presented, to the Board by the technical committee, during the presentation of the draft policy.

Because the PPRCN generates revenue based on the number of users. An accurate inventory of radios programmed and capable of utilizing the system must be maintained. This is accomplished through the assignment of Radio Ids. To facilitate less control over access of the system key tighter control over the issue of and addition of a Radio ID to the Zone Controller is necessary.

We propose this accomplished by changing the current system to a "*Positive Subscriber"* environment. This means a radio that ***does not*** have a pre-authorized Radio ID will not function on the system. To accomplish this the System Manager will have to be the only individual who is authorized to add a radio to the system. Stakeholder members will still maintain radio user/alias files.

PROCESS:

a) Positive Subscriber – Prior to Christmas Holidays
1) Review of ZC$ Radio ID and Radio Alias – SHM
2) Fix ZC$ of required radios – SHM
3) Report to System Manager – SHM
4) Change SHM permissions to add radios
5) Change System to Positive Subscriber

b) Approved Policy – Board – December Board Meeting

c) Requests for System Key submitted by SHM – By Second Week of December

d) Requests reviewed by Technical Committee and System Manager - December Meeting

e) Approval/Disapproval of Requests - December Meeting

f) System Key Provided – Completion of Positive Subscriber

g) Review and Report to PPRCN Board – NLT 90 days after issue.