Policies

Revised March 2, 2010

Contents:

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Proper Use of Network Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Operations & Maintenance**	Revised: **Sept. 14, 2009**	
Page: **1 of 2**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to define permissible communications and legitimate uses of the TOPAZ (**T**runked **OP**en **A**ri**Z**ona) Regional Wireless Cooperative (TRWC) network.

2.0 Owner

2.1. Administrative Manager

3.0 Applies To

3.1. Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network.

4.0 Background

4.1. TRWC is a radio communications network that supports both public safety and public service operations and operates using frequencies licensed for such purposes by the Federal Communications Commission. Proper use of the TRWC network is required to ensure the system is available to support the intended purpose.

5.0 Policy Statement

5.1. The TRWC network is authorized by the Federal Communications Commission to use frequencies allocated for public safety and public service operations. As such, use of the TRWC network shall adhere to the restrictions related to permissible use of the frequencies.

6.0 Supporting Rules

6.1. Communications must be directly related and necessary to the support of public safety and public services operations.

6.2. Communications involving the imminent safety of life or property have the highest priority.

7.0 Responsibilities

7.1. Area Managers and Members are responsible for ensuring that appropriate training plans incorporate information on proper use of the TRWC network.

7.2. Area Managers and Members are responsible for appropriate and authorized use of talkgroups.

7.3. Interoperable talkgroups or shared talkgroups are only used for the designated purpose and only when authorized in accordance with the TRWC Governance Agreement, section 6.4.1.

8.0 Conditions for Exemption or Waiver

8.1. None.

9.0 Applicable Procedures

9.1. Governance Agreement
9.2. Talkgroup Plan Approval Policy
9.3. Network Security (category) policies

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Maintenance & Support Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Operations & Maintenance**	Revised: **Sept. 14, 2009**	
Page: **1 of 6**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to establish the framework:

1.1.1. Necessary to identify, resolve, and report anomalies that occur within TRWC in such a manner as to minimize the operational impact to participating agencies and their subscribers.

1.1.2. Within which all maintenance activities pertaining to TRWC sites and facilities and TRWC infrastructure devices will be tracked and reported, including notification to Area Managers and Members of scheduled and unscheduled service affecting activities.

2.0 Owner

2.1. Administrative Manager

3.0 Applies To

3.1. Area Managers, Members, Associates, Interoperability Participants and Conditional Participants.

3.2. All personnel performing operations and planned or unplanned maintenance of the TRWC network infrastructure.

4.0 Background

4.1. The TRWC infrastructure is a critical enabling technology that supports public safety and public service operations with differing operational requirements. In anticipation of operational anomalies occurring within the network, and realizing that these anomalies must be triaged as expeditiously as possible, it is necessary to have policies in place that ensure network anomalies can be identified, reported, and resolved in a manner that minimizes the impact to Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network.

4.2. The operational stability of TRWC may be affected when the configuration of the TRWC network is altered. Proper notification of scheduled and unscheduled service affecting maintenance activities will allow Members and Area Managers time to make necessary preparations. Conversely, unauthorized disruptions in TRWC operations caused by the lack of notification will create safety issues that must be addressed by the Administrative Manager.

5.0 Policy Statement

5.1. The Administrative Manager will establish and maintain the necessary processes and procedures relative to internal activities and third party support providers to ensure that operational and technical anomalies relative to TRWC are identified, triaged, and reported in such a fashion as to minimize the operational impact.

5.2. Members and Area Managers will be notified of any scheduled and unscheduled service affecting maintenance activities that have potential impact to the operational capabilities of the network.

5.3. All planned and unplanned maintenance activities will be tracked and reported.

5.4. A repository for tracking and reporting maintenance management data will be maintained by the administrative manager.

6.0 Supporting Rules

6.1. At least twenty-four (24) hours advance notice will be given to Members and Area Managers prior to service affecting maintenance activities.

6.2. Service affecting maintenance activities not preceded by twenty-four (24) hours notice will be considered unscheduled maintenance.

6.3. Notification of unscheduled service affecting maintenance will be made to the Members and Area Managers as soon as practical.

6.4. Acceptable forms of notification would include phone, pager, e-mail, facsimile, or any other method as agreed to by the Administrative Manager, Area Managers, and Members.

6.5. At a minimum, the information contained in a notification will consist of:

6.5.1. A description of the planned maintenance activity.

6.5.2. The affected location(s) of the maintenance activity

6.5.3. Anticipated operational impact.

6.5.4. The scheduled start and stop time of the maintenance activity.

6.5.5. The name of department or organization responsible for performing the activity.

6.6. Contact information for Members, Area Managers, and their designated alternates to be used for notification purposes will be kept in a central location and accessible from the Administrative Manager's wide area network.

6.7. No service affecting maintenance activities will be conducted during agency planned special operations.

6.8. All maintenance activities will be tracked in a database in accordance with procedures developed by the Administrative Manager.

6.9. All components of TRWC managed by the Administrative Manager shall be entered into a database and tracked.

6.10. Database Backups

6.10.1. A multiple tape cycle backup method will be utilized for all database backups. The current backup tapes will be stored onsite at the server location. The backup prior to the current backup will be stored offsite at a secure location.

6.10.2. Manual backups will be performed when the databases have undergone significant changes.

6.11. Configurations files and event logs will be backed up as determined by the Administrative Manager.

7.0 Responsibilities

7.1. The management of the TRWC infrastructure is the responsibility of the Administrative Manager.

7.2. The Administrative Manager will establish on-call after-hour support for anomaly resolution.

7.3. The Administrative Manager will ensure that TRWC reporting activities for anomalies will be conducted seven (7) days a week and twenty-four (24) hours a day.

7.4. The Administrative Manager will:

7.4.1. Establish and maintain processes and procedures for operations and maintenance of the TRWC infrastructure.

7.4.2. Identify and resolve network anomalies. Field service personnel will be dispatched when problems cannot be resolved remotely.

7.4.3. Log problems and track them to closure.

7.4.4. Analyze all logged problems to ensure network performance standards are maintained.

7.4.5. Ensure that network log files are regularly reviewed and that cases are opened to resolve anomalies as necessary.

7.4.6. Provide system performance reports.

7.4.7. Maintain access to field replaceable units (FRUs) sufficient to mitigate equipment failures in a timeframe agreeable to TRWC Members.

7.4.8. Maintain current software licensing on all TRWC infrastructure components.

7.4.9. Maintain technical support necessary to operate, troubleshoot, and optimize the TRWC infrastructure.

7.4.10. Incident types, response times, and appropriate actions are defined by severity level in accordance with procedures established by the Administrative Manager.

7.4.11. Ensure that all operations and maintenance personnel, and third party support providers, are aware of this Maintenance & Support Policy; are trained in the appropriate processes, procedures, and response times; and have access to the necessary contact information to invoke various levels of support activities.

7.4.12. Perform scheduled maintenance on the TRWC infrastructure in a manner that is consistent with industry best practices and manufacturer recommendations.

7.4.13. Operate the TRWC network in accordance with the Network Security category polices.

7.4.14. Responsible for notifying the Members and Area Managers of scheduled and unscheduled service affecting maintenance activities.

7.5. Mesa PD is the point of contact for key management and encryption. Requests for key management and encryption support are to be submitted to Mesa PD during normal business hours if possible. After hours, the point of contact for emergency support of key management and encryption is Mesa PD dispatch.

7.6. Area Managers and Members are responsible for providing their own dispatch console maintenance.

7.6.1. Area Managers and Members are responsible for notifying the

Administrative Manager of maintenance activities on their consoles.

7.7. Area Managers and Members are responsible for communicating scheduled and unscheduled TRWC maintenance activities to their respective agencies and, if necessary, their respective dispatch centers.

7.8. Members and Area Managers are responsible for notifying Administrative Manager of the scheduling of planned special operations by their participating agencies.

8.0 Conditions for Exemption or Waiver

8.1. Routine maintenance activities will be exempt from the notification process.

9.0 Applicable Procedures and Reference Document

9.1. Change Control Policy

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Change Control Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Configuration Management**	Revised: **Sept. 14, 2009**	
Page: **1 of 4**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to ensure the proper change control processes and procedures are in effect to prevent unauthorized or harmful changes to the TRWC network infrastructure.

1.2. Changes will only be made to infrastructure configurations by following the procedures and approach described in this policy.

2.0 Owner

2.1. Administrative Manager

3.0 Applies to

3.1. All personnel attempting to make configuration changes to the production TRWC network infrastructure.

3.2. All TRWC network infrastructure components.

4.0 Background

4.1. Each component of the TRWC network infrastructure has a desired configuration that controls the operational capabilities of TRWC. Changes to the infrastructure configurations will be required from time to time. Because changes to infrastructure configurations have direct and immediate impact on the operational capabilities of the network, it is imperative that a policy exists to address how the configuration changes are requested, tested, approved, implemented and documented.

5.0 Policy Statements

5.1. Administrative control processes will be in effect at all times to ensure that all modifications to TRWC network infrastructure configurations are properly requested, analyzed, tested, approved, documented and implemented.

5.2. No service affecting modifications will be made to any TRWC infrastructure configurations without the review and approval of the Administrative Manager and in accordance with the “Maintenance & Support Policy.”

Supporting Rules

5.3. The Administrative Manager will coordinate all TRWC network infrastructure configuration changes.

5.4. All requests for network infrastructure configuration changes will be evaluated by the Administrative Manager for potential operational impact to subscriber agencies.

5.5. All network infrastructure parameter change requests will be reviewed by committees established by the Executive Director.

5.6. Each service affecting change to an infrastructure configuration will be thoroughly tested by the Administrative Manager.

5.7. Documentation shall be kept to provide an audit trail of the changes made to the network infrastructure configurations and to ensure that only the intended changes were made. Where applicable, output from configuration management software, electronic or hardcopy, shall be reviewed for accuracy and retained as part of the documentation package.

6.0 Responsibilities

6.1. The Administrative Manager will be responsible for providing the committees established by the Executive Director with an overview of all network infrastructure parameter changes that includes a description of the change, benefits of implementation, a risk assessment, proposed implementation schedule, options and alternatives relative to the change, and a recommended course of action.

6.2. The committees established by the Executive Director will be responsible for reviewing proposed changes to the TRWC network infrastructure parameter(s), assessing the impact of the change request, and providing feedback (recommendation) to Administrative Manager relative to the change request.

6.3. The Administrative Manager will be responsible for ensuring that all affected parties are aware of the approved configuration change request and participate in the testing process as appropriate.

6.4. The Administrative Manager will be responsible for collecting and retaining all documentation relative to the infrastructure change.

7.0 Conditions for Exemption or Waiver

7.1. Routine activities that result in changes to TRWC network infrastructure components such as adding subscribers to the UCS or other routine activities as determined by the Administrative Manager will be exempt from this policy.

7.2. During catastrophic events or emergency situations, immediate changes to the TRWC network infrastructure are authorized based on the judgment of the Administrative Manager, in consideration of all TRWC users, with

public safety considerations having the highest priority. The Administrative Manager will immediately notify the Executive Director, Members, and Area Managers, as time allows.

8.0 Applicable Procedures

8.1. Recommended form for Requests for Changes (following page of this policy)

8.2. Maintenance & Support Policy

Requests for Changes will take the following form:

REQUESTING AGENCY	
NAME OF REQUESTOR	
NEED BY DATE	
DESCRIPTION OF CHANGE	
PURPOSE OF CHANGE	
WORKGROUPS IMPACTED	
IMPACT EXPECTATION	
IMPLEMENTATION PLAN DEVELOPMENT (Task Definitions, Schedule, Responsibility, Recovery Strategy)	
ADMINISTRATIVE MANAGER RECOMMENDATION (section 6.1)	
FEEDBACK (RECOMMENDATION) FROM THE COMMITTEES ESTABLISHED BY THE EXECUTIVE DIRECTOR (section 6.2)	
ADDITIONAL COMMENTS	

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Talkgroup Plan Approval Policy**	
Owner: **See Below**	Created: **Sept. 14, 2009**	Applicability: **See Below**
Category: **Configuration Management**	Revised: **Sept. 14, 2009**	
Page: **1 of 2**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to establish a process for talkgroup plan approval.

2.0 Owner

2.1 Administrative Manager

3.0 Applies To

3.1 Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the TOPAZ (**T**runked **OP**en **A**ri**Z**ona) Regional Wireless Cooperative (TRWC) network.

4.0 Background

4.1 A talkgroup is a defined organizational grouping of radio users that need to communicate together. When two or more radio users select the same talkgroup on their radios, all radio users with that talkgroup selection hear the transmitted audio. A talkgroup plan is the summary of all defined radio talkgroups. This plan is then used to develop the radio template which is the programming data for the individual radios.

5.0 Policy Statement

5.1 As talkgroup plans are designed to support public safety and public service operations for the Members, and have a direct impact to TRWC system performance, the Administrative Manager will review and approve all talkgroup plans and proposed changes.

6.0 Supporting Rules

6.1 Each Area Manager's and Member's agencies are responsible for development of their talkgroup plans.

6.2 As the number of talkgroups has a direct impact to system performance, all proposed talkgroup plans should consider possible impacts to system loading and performance.

6.3 Each agency using TRWC will develop a preliminary talkgroup plan that considers internal business operations and any requirements for communications with other TRWC entities.

6.4 Upon completion of the preliminary talkgroup plan, the agency shall submit the preliminary plan to the Administrative Manager for technical and operational analysis.

6.5 The Administrative Manager will complete a technical review and provide the committees established by the Executive Director with an analysis on system performance related to the proposed talkgroup plan.

6.6 The committees established by the Executive Director will consider the preliminary talkgroup plans and all supporting information and recommend approval of the request or make a recommendation for changes to the requesting agency.

7.0 Responsibilities

7.1 The Administrative Manager is responsible for maintaining a database of all approved talkgroup plans.

8.0 Conditions for Exemption or Waiver

8.1 None

9.0 Applicable Procedures

9.1 Governance Agreement, section 6.4.1

TOPAZ REGIONAL WIRELESS COOPERATIVE	**System Key Control Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Network Security**	Revised: **March 2, 2010**	**REVISION 1**
Page: **1 of 4**	Last Review:	

1.0 Purpose

1.1. The purpose of this policy is to establish the controls for the TRWC System Key used for subscriber unit programming.

2.0 Owner

2.1. Administrative Manager

3.0 Applies To

3.1. Anyone that has access to the TRWC subscriber programming software.

4.0 Background

4.1. TRWC is a radio communications network that provides services and features to radio users through the programming software of the subscriber radios. Programming of the subscriber radios is controlled by an electronic "System Key." As this programming application directly affects the TRWC public safety and public service department operations it is important that the System Key is protected from potential security related risks that can cause disruptions or anomalies to subscriber operations.

4.2. The System Key may take the form of a "software" System Key or an "Advanced" System Key ("ASK"). The ASK is comprised of two components, a "parent" key and "child" key(s). There is only one parent key per system, but there may be multiple child keys per system.

4.3. The System Key must be programmed into any subscriber unit that operates directly on TRWC. These subscriber units include all Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants, and could also include radio units from other entities that are given access rights to use TRWC.

4.4. TRWC public safety departments have operational requirements and mutual aid agreements that require they interoperate with non-TRWC entities. Direct interoperability (automatic unit to unit) is supported by programming non-TRWC subscriber equipment with the TRWC System Key. Please refer to section 4.1.5 of the Governance Agreement.

4.5. The risk of inaccurate programming substantially increases when multiple entities are allowed access to and use the System Key to program

subscriber units. This risk translates into an increase in subscriber radio operational anomalies and the associated administrative/maintenance activities. There is also an increased risk of possible unauthorized transmissions, interference or monitoring of public safety radio communications channels.

5.0 Policy Statement

5.1. Anyone that has access to the TRWC subscriber programming equipment shall at all times employ appropriate operational and network security practices, as adopted by the Administrative Manager, to protect TRWC users from programming errors that could potentially cause disruptions or failures in service.

5.2. The Administrative Manager will control the TRWC System Key. The TRWC software System Key and the ASK parent key will not be released to Area Managers, Members, Associates, Interoperability Participants, Conditional Participants, or their Contractors.

5.3. An ASK child key will be released to Area Managers, Members, Associates, Interoperability Participants, or Conditional Participants in accordance with the provisions described herein.

5.3.1. A separate ASK child key and request form will be required for each programming template to be used with the ASK child key (i.e. law enforcement, fire, public works).

6.0 Supporting Rules

6.1. The Administrative Manager will provide all routine and emergency TRWC radio programming services for the Area Manager, Members, Associates, Interoperability Participants, and Conditional Participants as defined in the TRWC Governance Agreement.

6.2. Requests for programming of the TRWC System Key into non-TRWC radios shall be made by the appropriate representative of the requesting agency to the Executive Director.

6.3. The Administrative Manager will provide, upon approval by the Executive Director, programming services for authorized non-TRWC radios for interoperable service as defined in section 4.1.5 of the TRWC Governance Agreement.

6.4. Any breaches in TRWC System Key use shall immediately be reported to the Administrative Manager and Executive Director who shall take immediate steps to minimize the danger to the operational capabilities of TRWC.

6.5. An ASK child key will be issued upon acceptance of a written request by a Representative to the Executive Director containing the information on the “Advanced System Key (ASK) Child Key Request” form.

6.6. The following rules apply to the issuance of an ASK child key:

6.6.1. Adherence to this Policy, in particular the need to safeguard the ASK child key and report the loss of an ASK child key as required in section 6.4.

6.6.2. Agreement to pay the hardware cost of the ASK child key and for the Administrative Manager's time to create the ASK child key and associated template development.

6.6.2.1. A time & material "Two-Way Radio Equipment Maintenance Agreement" with the City of Mesa is required to enable billing of the costs above (**not** a monthly recurring fee).

6.6.3. Timely notification to the Administrative Manager if a radio programmed with their ASK child key is missing, lost, stolen, destroyed, or otherwise rendered inoperable.

6.7. Upon notification by the Executive Director that a written request for an ASK child key has been accepted, the Administrative Manager will create an ASK child key and arrange for receipted transfer to the responsible party.

6.7.1. The Administrative Manager will create an ASK child key specifying the radio identification number (ID) range and set the permissions (such as talkgroups, functions, templates) for the requestor to program radios on the TRWC network.

6.7.2. The Administrative Manager will work with the responsible party to develop a radio programming template for use with the ASK child key being issued.

6.7.3. The ASK child key will be set to expire 18 months after the date the ASK child key is created. An expired ASK child key must be replaced, by initiating the process described in section 6.5, above.

6.7.4. The ASK child key will be issued with password protection enabled. The password will be communicated to the responsible party.

6.7.5. The responsible party is required to notify the Administrative Manager of the radio identification number(s) (ID) and radio serial numbers to be enabled in the infrastructure before the radio will be operational on the TRWC network.

6.8. The TRWC reserves the right to audit the ASK child key, radio identification numbers (IDs), and associated templates.

7.0 Responsibilities

7.1. The Administrative Manager is responsible for the development of internal controls for protection of the TRWC System Key.

7.2. The Administrative Manager or designee is responsible for monitoring issues related to use of the System Key, and to report actions involving misuse of the System Key to the Administrative Manager and Executive Director for resolution.

8.0 for Exemption or Waiver

8.1. None

9.0 Applicable Procedures

9.1. TRWC Governance Agreement
9.2. Recommended Form for Advanced System Key (ASK) Child Key Request
9.3. City of Mesa Two-Way Radio Equipment Maintenance Agreement

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Advanced System Key (ASK) Child Key Request**	
Owner: See Below	Created: **March 2, 2010**	Applicability: See Below
Category: **Network Security**	Revised:	**ASK CHILD KEY REQUEST FORM**
Page: **1 of 1**	Last Review:	

To be completed by Advanced System Key (ASK) Child Key Requester
(all lines below are required to be filled in)

Organization: _____

Representative Name: _____

Date of Request: _____

Responsible Party Information:

Name: _____

Job Title: _____

Mailing Address: _____

_____

City, State, & Zip Code: _____

Telephone Number: _____

E-mail Address: _____

Representative acknowledges receipt of the attached TRWC System Key Control Policy.

Signature of Representative: _____

To be completed by the TRWC Executive Director

Signature & Date for Acceptance of ASK Child Key Request: _____

To be completed by Administrative Manager

ASK Child Key Created Date/Expiration Date: _____/_____

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Password Administration Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Network Security**	Revised: **Sept. 14, 2009**	
Page: **1 of 3**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to establish a standard for the creation of passwords for access to the TRWC Network in order to prevent unauthorized read or write access.

2.0 Owner

2.1. Administrative Manager

3.0 Applies To

3.1. All personnel who have or are responsible for an account, or any form of access that supports or requires a password.

4.0 Background

4.1. There are multiple software applications, protected by password access only, available in the TRWC system. Access privileges provide critical configuration and security information that make it imperative to control the viewing, modification, and potential dissemination of this information. Unauthorized access, whether malicious or unintentional, must not be permitted.

5.0 Policy Statement

5.1. The Administrative Manager will establish and maintain the necessary processes and procedures to ensure that passwords to include the read, write, and executable functions of the TRWC system applications, components and interfaces are restricted to authorized users.

6.0 Supporting Rules

6.1. Users will not loan, share, divulge, or otherwise make accessible their password(s) to other individuals. All passwords are to be treated as sensitive and confidential information.

6.2. Passwords must not be inserted into email messages or other forms of electronic communication.

6.3. TRWC passwords should contain both upper and lower case letters when applicable.

6.4. TRWC passwords should have numbers (0-9) and letters.

6.5. TRWC passwords must be at least eight characters in length.

6.6. TRWC passwords must not be based on personal information, names of family, etc.

6.7. Derivatives of user-IDs and common character sequences such as "123456" must not be employed.

6.8. Personal details such as license plate, social security number, or birthday must not be used. Passwords created by using a proper name, geographic location, common acronym, or slang, must be made unique by inserting special characters or through combinations of characters or words that would be difficult to duplicate.

6.9. TRWC users must not create passwords that are identical or substantially similar to passwords they previously employed.

6.10. TRWC passwords should never be written down or stored on-line.

6.11. TRWC users must not use the same password for TRWC accounts as for other non-TRWC access.

6.12. TRWC users must not use the “Remember Password” feature of any TRWC applications.

6.13. The interval for changing passwords will be set at a maximum of 35 days.

6.14. New passwords issued must be valid only for the authorized user’s first on-line session. Upon initial access, the user must choose another password before any other work is done.

6.15. If an account or password is suspected of having been compromised it must be reported to the Administrative Manager immediately.

7.0 Responsibilities

7.1. The Administrative Manager will publish and provide a recommended form for Electronic Access Requests to all requesting agencies. All access requests will be subsequently reviewed and a response provided to the requestor in a timely manner.

7.2. The Administrative Manager will conduct a password audit and provide the Executive Director, on a regular basis, with user profile reports showing personnel access to key infrastructure components, user databases, component operating systems and system interfaces.

7.3. The Administrative Manager will ensure that all TRWC personnel are aware of the Password Administration Policies.

7.4. The Administrative Manager will monitor, though manual audits of log files or automated software, any access attempts deemed of a suspicious or malicious nature. Suspicious or malicious access attempts will be reported to the Executive Director.

7.5. The Administrative Manager will maintain all electronic access request records.

7.6. The Administrative Manager will maintain a centralized user access control list to determine, audit and report who is authorized to access the network.

7.7. Personnel and contractors involved in the support of TRWC will acknowledge the receipt, comprehension and adherence of the TRWC Password Administration Policies by signature which will be returned to the Administrative Manager.

8.0 Conditions for Exemption or Waiver

8.1. In the event an emergency, the Administrative Manager has the capability to provide immediate access to personnel on a case-by-case basis.

9.0 Applicable Procedures and Reference Documents

9.1. Recommended form for Electronic Access Requests

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Access to Administrative Functionality Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Network Security**	Revised: **Sept. 14, 2009**	
Page: **1 of 2**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to limit electronic access to the TRWC administrative functions to prevent unauthorized administrative changes and provide a method for user accountability.

2.0 Owner

2.1. Administrative Manager

3.0 Applies to

3.1. All personnel attempting to make modifications to TRWC user databases, infrastructure programming, and component operating systems.

4.0 Background

4.1. There are multiple software tools available in the TRWC network that provides useful administrative functionality to network management and operations and maintenance personnel. The administrative privileges also provide critical configuration and security information that make it imperative to control the read and write functions of files and potential dissemination of this information.

5.0 Policy Statement

5.1. Administrative access to include the read, write and executable functions of the TRWC system administrative tools is restricted to users authorized by the Administrative Manager.

6.0 Supporting Rules

6.1. Personnel with electronic access to the administrative functions of TRWC are required to have a current, signed recommended form for Electronic Access Request on file with the Administrative Manager. These documents may be subject to renewal at regular intervals.

6.2. The Administrative Manager will review all request for electronic access using appropriate justification and verification processes.

6.3. Administrative users will be granted levels of access (read, write, execute) to programs based on the minimum necessary to perform their job.

6.4. If any person discovers they have inadvertently been allowed access to a programming function not required to perform their job or are uncertain

about their privilege level, they will report it to the Administrative Manager immediately.

7.0 Responsibilities

7.1. The Administrative Manager is responsible for ensuring the approved administrative access to the system is currently required to perform personnel work duties and the type of access required matches the current privilege level.

8.0 Conditions for Exemption or Waiver

8.1. None

9.0 Applicable Procedures

9.1. Recommended form for Electronic Access Requests

9.2. Remote Access Policy

9.3. Password Administration Policy

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Remote Access Policy**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Network Security**	Revised: **Sept. 14, 2009**	
Page: **1 of 3**	Last Review: **Sept. 14, 2009**	

1.0 Purpose

1.1. The purpose of this policy is to minimize the risks associated with provisions for remote access to the TRWC network.

2.0 Owner

2.1. Administrative Manager

3.0 Applies To

3.1. Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network, and all contractors.

3.2. This policy covers all TRWC system software and infrastructure components that are accessible via remote access including, but not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, terminal server connectivity, or remote control software.

4.0 Background

4.1. The TRWC system is comprised of a multitude of components that inherently have the capability for a user to communicate with the target component from a remote location via a pre-determined login/password routine. In some instances this capability may allow off-site personnel to perform diagnostics and resolve system trouble without traveling to the physical location.

5.0 Policy Statement

5.1. Remote access to TRWC is prohibited unless expressly permitted by the Administrative Manager.

6.0 Supporting Rules

6.1. All Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network and contract vendors are required to submit in writing to the Administrative Manager, in advance, their requests for remote access to TRWC using the recommended form for Electronic Access Requests (or equivalent) including the general functions and expected duration of the tasks to be performed via the remote connection.

6.2. All remote access request responses from the Administrative Manager will be returned to the requesting organization with an explanation for denial or approval.

6.3. Remote connections are not permitted to retrieve files from inside TRWC.

6.4. Any computer permitted remote access to the TRWC network requires certification to the Administrative Manager that the computer has the latest virus definitions, operating system patches, and is in compliance with all security configuration requirements.

6.5. Any computer used to remotely access the TRWC network and physically connects to other public or private networks (i.e. - VPN) shall be capable of using encryption.

6.6. Individuals or their agency representative will promptly notify the Administrative Manager whenever any user who has been granted remote access no longer requires access to the TRWC network or TRWC related equipment.

6.7. Any computer with the ability to access TRWC and other non-TRWC networks must be configured with a personal firewall, virus protection software, or equivalent to protect against viral propagation between networks.

6.8. Any individual or company granted TRWC remote access will not share, publish, or divulge by any means, connection information, including but not limited to, modem numbers, ISDN numbers, IP addresses, access codes, passwords, logins, and secure tokens.

7.0 Responsibilities

7.1. The Administrative Manager will establish and maintain the necessary processes and procedures to prohibit, unless expressly permitted, remote access to TRWC infrastructure components and system software to include, but not be limited to, network transport, RF infrastructure, site equipment, the Private Radio Network Management Suite (PRNM) and the Core Security Management Suite (CSMS).

7.2. The Administrative Manager will ensure that a centralized user access control list will be maintained to determine, audit and report who is authorized to remotely access TRWC.

7.3. The Administrative Manager will conduct a remote access audit to generate and maintain user profile reports showing personnel, including vendors, with remote access to key infrastructure components, system software, user databases, and component operating systems.

7.4. The Administrative Manager will notify the Executive Director of any remote access attempts deemed of a suspicious or malicious nature.

7.5. The Administrative Manager will ensure that any changes to firewall configurations and/or access control lists will be reviewed and approved.

7.6. The Administrative Manager will ensure that all Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network, and contract support providers, are aware of the Remote Access Network Policies, and have access to the necessary contact information to request remote access for their personnel.

8.0 Conditions for Exemption or Waiver

8.1. None

9.0 Applicable Procedures and Reference Documents

9.1. Recommended form for Electronic Access Requests

TOPAZ REGIONAL WIRELESS COOPERATIVE	**Recommended Form for Electronic Access Request**	
Owner: See Below	Created: **Sept. 14, 2009**	Applicability: See Below
Category: **Network Security**	Revised: **Sept. 14, 2009**	
Page: **1 of 1**	Last Review: **Sept. 14, 2009**	

To be completed by Electronic Access Requester

Name _____

Agency/
Department _____

Date _____

Functionality Requested _____

_____

Reason for Request _____

_____

Duration Required _____

Request for Access and
Acknowledgement of TRWC
Password Administration Policy _____

To be completed by Administrative Manager

Access Granted Date: _____