Title:	P25 System Management Access Policy for External Agencies	SOP No:	ITS-RADIO-009
Revision:	1.2	Effective Date:	December 18, 2018
Owner:	Manager Wireless Communications	Department:	IT Solutions

System Management Access Policy for External Agencies

1 Purpose

Establish a system management access policy that describes the capabilities that may be accessible to external agencies that utilize the public safety radio system that provides communications for first responders across much of North Central Texas network for communications.

2 Scope

This policy applies to all external agencies connecting to the Radio System network irrespective of network connection type whether infrastructure, console or subscribers only.

3 References

- ITS-RADIO-007: Security Policy for External Customers
- ITS-RADIO 005: Subscriber Template Management
- ITS-RADIO-008: Network Security Operation System Upgrades and Patches
- ITS-RADIO-010: System Management Infrastructure Externals
- ITS-RADIO-011: System Management Subscriber Externals

4 Conditions for Exemption

External agencies that do not require any Network, Subscriber or IV&D Management capabilities.

Exceptions to the policy must be approved by the Senior Manager over Wireless Communications.

5 Justification

Defined guidelines and responsibilities for system, network, subscriber and infrastructure management provides specific information to external agencies on the features and functions that may be accessible on the Radio System network. This policy also allows the City to monitor and track network access for security purposes but also ensure network management licensing is appropriate and remains adequate to support overall system usage.

6 System Management Access and Responsibilities

6.1 System Management Access Protocol

External agencies may request system management access to the Radio System network by contacting the City of Fort Worth Communications Manager prior to purchasing equipment. Each customer's individual operational requirements will be discussed as well as the status of existing CFW hardware/software/licensing environment.

System management equipment, both hardware and software has specific operational and licensing limitations that must be managed closely by the CFW to ensure sufficient resources are available for all users on the network. Therefore, the CFW will evaluate each external agencies needs and establish a specific system management access protocol at the time of the request based on the guidelines in this policy.

6.2 System Management Security

The CFW will use security groups to manage access to the Radio System network specific to each external agency's operational requirements. Access rights will only be granted to the specific equipment, hardware and software necessary to the external agencies needs for system management. Where applicable, network partitions will be applied to further control network access and protect overall security of the Radio System network.

External agencies must establish user login accounts that are customized and independently assigned on an as needed basis only. Recommendations for login and password policies are described in policies Radio-007 and Radio-008.

Also, external agencies must not add, remove or modify the software, configuration, equipment programming or parameters of network management equipment used to connect to the Radio System network.

6.3 Network Management Responsibilities

Once approved, external agencies are responsible for the procurement, installation and maintenance of network management equipment and software licensing (if necessary) that is purchased for connectivity to the Radio System network. Per the external agency's ILA with the CFW, network management equipment must be secured, configured and accessible per the guildeines established in 6 dictating authorized use and specific usage. Please also refer to policies Radio-007 and Radio-008 for specific security and network guidelines.

6.4 Network Management Applications

This section provides a description of the zone and system level applications that may be accessible to external agencies.

Examples of Network Management features and functions are:

- Systemwide Parameters
- Infrastructure and equipment operational parameters
- Network Fault Management
- Security groups
- Login user accounts

Zone Level Performance and Fault Management Applications

Zone level performance and fault management applications may be accessible to customers with Master Switches specific to their operational needs as discussed in 6.1

Zonewatch is utilized exclusively by the Cities of Fort Worth and Irving as Master Switch operators to display real-time communications activity and track network capacity, performance and resource loading in their respective zones.

UEM (Unified Event Manager) allows zone level system management of infrastructure devices in graphical format including site control, reporting, alarms and radio status. The City of Fort Worth and Irving are licensed for UEM access as Master Switch operators.

MOSCAD Network Fault Management (NFM) Server allows system level management of alarms from devices and transmits the information to the Unified Event Manager (UEM). NFM

Workstation access may be accessible to Master Switch Customers with infrastructure connections to the Radio System network.

System Level Configuration Management Applications

System level configuration management applications may be accessible to Master Switch customers with infrastructure and/or Consoles based on their specific operational needs as discussed in 6.1

Unified Network Configurator (UNC) is a single application that allows configuration of all radio network and transport devices on the system.

User Configuration Manager (UCM) is a communications management tool that allows configuration and control of consoles and subscribers. Features include manipulation of security groups, partitioning, fleet management of talkgroups and multigroups and user profiles.

Performance Management Applications

Performance management applications may be accessible to Master Switch customers with infrastructure and/or Consoles based on their specific operational needs as discussed in 6.1

Radio Control Manager (RCM) is a capability used to monitor and manage radio incidents, issue commands and query the system database for specific information such as dynamic regrouping, selective inhibit and emergency alarm display.

Subscriber Alias Management

Subscriber alias management applications may be accessible to customers with subscribers and/or infrastructure and consoles based on their specific operational needs as discussed in 6.1

The CFW manages and maintains subscriber aliases on the network. Alias Management may be accessible to external agencies that require the ability to modify their own alias database. However, external agencies who begin administering and maintaining their own aliases must continue to manage their databases on an ongoing basis. Please refer to ITS-RADIO-010 and ITS-RADIO-011.

Title:	P25 System Management Access Policy for External Agencies	SOP No:	ITS-RADIO-009
Revision:	1.2	Effective Date:	December 18, 2018
Owner:	Manager Wireless Communications	Department:	IT Solutions

6.5 Integrated Voice and Data (IV&D) Applications

External agencies that intend to implement IV&D on their infrastucture and consoles for over-the-air Programming (OTAP) and/or over-the-air rekeying (OTAR) must also discuss their specific requirements with CFW per Section 6.1 of this policy. Radio-004, Radio-007 and Radio-008 policies provide specific security and encryption guidelines with regards to OTAP and OTAR.

The CFW also manages the P25 radio network's capacity, hardware, software and licensing with regards to total customer enterprise network (CEN) connections and IV&D. Its vital that these parameters are closely monitored and evaluated as IV&D external agencies are added to the network.

OTAP Networks

External Agencies with OTAP will be managed by the CFW. If customers implement their own Presense Notifier (PN) Server, they will then be responsible for managing their own programming per policies Radio-007 and Radio-005.

OTAR Networks

External Agencies using AES Encryption and OTAR on their infrastructure and console networks without a Key Management Facility (KMF) will be managed and monitored by the CFW.

If a KMF is implemented, the external agency will have access to their own OTAR client and is responsible for managing their own encryption keys as specifically documented in Radio-004.

7 Supporting Documentation

Each external agencies specific executed ILA Agreement with the City of Fort Worth.

Title:	P25 System Management Access Policy for External Agencies	SOP No:	ITS-RADIO-009
Revision:	1.2	Effective Date:	December 18, 2018
Owner:	Manager Wireless Communications	Department:	IT Solutions

Version Control

Version	**Date**	**Description**	**Author**
1.0	8/1/2014	Original version	Abinta Khan
1.1	12/20/16	Changed Radio Services to Wireless Communications, FW P25 Radio System to Fort Worth Regional Radio System, Document formatting	Kim Smith
1.2	12/18/18	Changed FWRRS to Public Safety	Larry Crockett