Title:	P25 Network Security O/S Patches and Upgrades	SOP No:	ITS-RADIO-008
Revision:	1.0	Effective Date:	August 1, 2014
Owner:	Manager - Radio Services	Department:	IT Solutions

P25 Network Security O/S Patches and Upgrades

1 Purpose

This policy outlines network security maintenance requirements for external agencies that connect to the City of Fort Worth network for primary radio communications.

2 Scope

This policy applies to all external agencies with console and/or radio networks connecting to the City of Fort Worth P25 network.

3 References

- ITS-RADIO-007 Security Policy for External Customers

4 Conditions for Exemption

Exceptions to the policy must be approved by the Senior Manager over Radio Services.

5 Justification

Equipment, structures, operating systems, hardware and software utilized by external agencies to connect to the City of Fort Worth P25 network must be maintained to protect the security, performance and functionality of the network for all entitites.

6 Subscriber Template and Configuration Programming Rules

The CFW recommends that all External Agencies establish a documented Cybersecurity Policy that incorporates network security maintenance requirements. This policy should be enforced and the staff must be held accountable for compliance and any security breaches.

6.1 Network Maintenance Requirements

All security structures utilized to connect to the CFW network must have current and/or vendor approved versions, industry standard supported and hardened operating systems and endpoint security software. The appropriate versions will be coordinated with CFW and Motorola if the equipment is under a Software or System Upgrade Agreement (SUA-2). All hardware and software should have current maintenance and support agreements in place.

External Agencies must maintain all network security equipment used to connect to the City of Fort Worth network in one or more of the methods described below:

- **System Maintenance Agreements**
  External Agencies with existing Operation and Maintenance Agreements with their radio system and/or console vendor may incorporate network security equipment that complies with section 6 of this policy.

- **Third Party Maintenance Agreements**
  External Agencies may establish individual maintenance agreements with the third party vendors, manufacturers and/or service providers of the specific network security equipment described that complies with section 6 of this policy.

- **External Agency Maintenance**
  The External Agency may also individually maintain the network security equipment as described in section 6 of this policy.

6.2 Hardware and Operating System Maintenance

External Agencies are required to maintain hardware and operating systems in accordance with industry standard supported systems.

The CFW also recommends the following guidelines per AR-D5 section 9.2.1 of the City's IT Security Policy.

- **Passwords and Accounts**
  - Passwords should comply with Appendix 1 of AR-D5, which defines the City of Fort Worth Password Policy and is referenced in Section 7.
  - Suggested rules are that passwords and accounts must not be shared across users, all access granted must be limited to that which is specifically required and usage should be tracked and documented to track individual user activity. All passwords should be changed from their default values before activation as "live". Guest or anonymous accounts should be disabled or removed.
  - Passwords should follow Microsoft best practices for password protection which is also referenced in Section 7 of this policy.

- **Security Patches**
  Operating system patches must be performed on an established maintenence schedule to protect against security breaches and loss of service that may result.

- **Logon Banners**
  The CFW implements logon banners on all operating systems at the start of the logon process and also recommend this procedure for External Agencies. Logon banners inform users that the asset and application accessed is the property of the specific agency who owns it, should only be used by those authorized and that it is being monitored.

6.3 Endpoint Security Software

External Agencies must maintain endpoint security software to protect their security structures and subsequently the CFW P25 network for all users against intrusive programs designed to disable, modify or self-replicate and propagate. The following measures must be applied to all relevant security assets AR-D5 section 9.2.2 of the City's IT Security Policy.

- All security structures used to connect to the CFW P25 network must have endpoint security software correctly installed, configured and updated. Endpoint security software must be enterprise grade.

- Updates to endpoint security software must be applied as soon as they are available or in accordance with their manufacturer's alternate schedule if agreed upon in advance with the CFW.

- All USB ports should be software and hardware locked down and only opened for maintenance purposes. External USB or other devices must not be connected to security structures that are used to connect to the CFW P25 network.

- All files downloaded from external networks onto security structures must be scanned by the endpoint security software.

6.4 Auditing and Logging

The CFW implements a logging and auditing process in compliance with AR-D5 section 9.2.3 of the City's IT Security Policy. Secure logging and auditing ensures correct use of security structures, flags potential problems for resolution and maintains a record that may be accessed to analyze an incident.

External Agencies are encouraged to maintain a logging and auditing process that follow the guidelines below:

- Secure logging of system activity for "system administrator" user accounts and significant relevant events such as password guessing attempts, attempts to use priveleges not authorized, modifications to systems or software and changes to groups or accounts.

- Secure logging of key user activity information such as session activity, user accounts, login and logout dates and times, applications utilized, changes to applicaton system files, changes to user priveledges and system startup and shutdowns.

- IT Asset Managers are responsible for establishing appropriate retention timeframes for secure logging. Stored logs should be secure, inaccessible and uneditable except by authorized users.

7 Supporting Documentation

Information Technology Security **AR-D5** February 8, 2010 Appendix 1 City of Fort Worth Password Policy
AR-D5 Appendix 1

CJIS Requirements
http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

Microsoft Password best policies
http://technet.microsoft.com/en-us/library/cc784090(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx

Title:	P25 Network Security O/S Patches and Upgrades	SOP No:	ITS-RADIO-008
Revision:	1.0	Effective Date:	August 1, 2014
Owner:	Manager - Radio Services	Department:	IT Solutions

Version Control

Version	**Date**	**Description**	**Author**
1.0	8/1/2014	Original version	Abinta Khan