Title:	P25 Security Policy for External Customers	SOP No:	ITS-RADIO-007
Revision:	1.0	Effective Date:	August 1, 2014
Owner:	Manager Radio Services	Department:	IT Solutions

Security Policy for External Customers

1 Purpose

This security policy outlines the requirements for external agencies to gain access to the City of Fort Worth radio system. It also specifies the equipment, configuration and operating procedures necessary to connect to the network.

2 Scope

This policy applies to all external agencies connecting to the City of Fort Worth P25 network irrespective of network connection type whether infrastructure, console or subscribers only.

3 References

- Radio 008: Network Security Operation System Upgrades and Patches
- Radio 004: Encryption Management
- Radio 005: Subscriber Template Management

4 Conditions for Exemption

None.

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

5 Justification

Security policy based on the City's IT Security Policy AR-D5 and industry standards provide specific guidance for external agencies that protect and enhance the security, performance and functionality of the network for all entities. It also ensures that external agencies have adequate time for planning, budgeting and maintenance of their equipment and responsibilities.

6 Security Policy for External Agencies Guidelines

The policy guidelines described in this section apply to all agencies and entities. The CFW recommends that all external agencies establish a documented Cybersecurity Policy that is enforced and staff be held accountable for compliance and any security breaches.

6.1 Information Technology Security Contacts

The CFW Helpdesk should be contacted for all support requests as described on the first page of this policy.

6.2 CFW and External Agency System Requirements

External Agencies are required to provide a single point of contact for connectivity and security that may be contacted by the CFW Radio Services Manager if necessary.

6.3 Security Assessments

External Agencies connecting to the CFW network must comply with CJIS requirements and regulations. Internal CFW Departments are also required to complete Security Assessments as specified in section 8.1 of **AR-D5**.

6.4 IT Asset Classification and Risk Mitigation

CFW network equipment such as firewalls, routers, LAN switches and other which is utilized for external connectivity via the Radio Network (RNI) or Customer Enterprise Network (CEN) is considered Class A as defined in 8.2.1 of **AR-D5**. Categorization of information should be conducted in each organization on the basis of its sensitivity per the CIS and the CFW IT Security Policy. As such, this equipment must be assessed annually for protection and security. The CFW recommends that External Agencies conduct security assessments to ensure protection of these critical assets.

6.5 IT Security Breach Incident Response

Additionally per 8.3 of AR-D5, a risk mitigation plan must be developed for equipment classified as Class A. The CFW recommends that external agencies develop an IT security breach incident response plan per the guidelines outlined in Figure 1 below.

IT Security Breach Risk Mitigation

Prevention of security breaches is the first step to mitigating the risks of an IT security breach as outlined in this policy and **Radio-008**. External customers are encouraged to implement and actively enforce an IT security breach risk mitigation plan as part of their IT security policy.

Recommended practices for securing IT security systems:

- Risk Management is comprised of periodic risk assessments which evaluate the probability of the loss from occurring and identifying system vulnerabilities which would be targeted should they occur. The process of taking action to identify, avoid or eliminate the risks must be performed on an ongoing basis.
- Hardened network and security systems
- Malware security software
- Security team ongoing training

An incident detection and response team should be established with clearly identified services and communication protocols. Additionally, preplanned and documented policies and procedures should be written to prevent the occurrence and reduce frequency of security breaches. Detailed procedures should be drafted and customized to address incidents that are known and specific but also unknown and general with priority levels assigned. Lessons learned from resolved security incidents should be reviewed, discussed and then used to update the IT security risk mitigation plan on a dynamic basis.

Some examples of incidents that should be addressed per NIST are; external/removable media, attrition using brute force to target systems, web based or email based attacks, improper usage, loss or theft of equipment and others.

Detect and Analyze Security Breach Incident

When an incident is detected or reported, it must immediately be reported via an ITSM Helpdesk ticket and also to the IT Security Manager. External users experiencing a security breach must follow the same process. The team identified in the IT security breach risk mitigation plan must first respond quickly to evaluate the incident, its scope and impact and assign a priority level based on known information and functional impact. The initial assesment must also determine if a quick recovery solution is possible, or else develop a strategy for immediate containment.

The IT security breach incident response team's knowledge and experience coupled with technological tools, resources and established policies are key factors in detecting and addressing an incident.

SANS recommends that the IT security breach response team focuses on five critical areas once an incident occurs:

1. Immediately identify the systems and data that are affected to the highest extent possible.
2. Evaluate how the security breach occurred using automatic and manual methods.
3. Possible sources have the incident whether external, internal, targeted or general.
4. Once resolved, confirm that the threat is fully remediated or if any remnants remain. In order to successfully confirm that the security breach is indeed over, continual monitoring is necessary as well as absolute confidence that the source was identified.
5. Continual risk management of possible security vulnerabilities, threats and closed security incidents is necessary to continuously evaluate the network security and resilience of networks against future attacks.

Intrusion Detection is the first step in the process and may involve the use of automatic security detection technologies and manual means such as reported problems or unusual activity detected by a security team member. Ongoing monitoring to alert and communicate the occurrence of an incident should also be done. Some examples per NIST may be areas of vulnerability identified in web server log entries, direct threats from an organization or individual or new announcement of a virus or other threat.

Examples of automatic security detection per NIST:

- Intrusion Detection Prevention Software and/or Security Information and Event products that generate alerts
- Malware prevention software such as antivirus, antispam and other
- File integrity checking software that detects changes to important files during incidents
- Third party monitoring services
- Operating system, network device logs and traffic flow information
- ITSM Helpdesk reported problems

The team should also remain aware of new threats and advisories by monitoring IT security incidents on a global level, IT vulnerabilities databases and other means. The IT security breach response team must maintain appropriate and relevant skill sets, education and knowledge about threats on a continual basis. A means of information sharing and coordination is recommended when incidents occurs which should be documented as part of the response plan.

Specific equipment may be designated, or else set aside specifically for handling IT security breaches such as logging and recording devices, backup and removable media, spare

workstations, portable printers, packet sniffers and protocol analyzers, security software and/or other evidence gathering equipment and tools.

Contain, Resolve and Recovery Stage

Following the initial analysis, the team must then perform a deeper investigation using manual and automatic methods to determine the incidents direct and indirect affect on IT security, hardware, software and systems. All evidence and information should be documented and logged. Possible causes of the incident should be identified. If the incident is not yet resolved, a permanent solution is finalized and agreed upon by consensus from the IT security breach response team. If the event remains unrecoverable, a permanent containment strategy must be implemented including documented information on its expected security impacts, any loss or reduction in service and functional or operational effect. The expected timeframe for recovery should also be documented.

Per NIST, functional impact may be categorized by severity level. Also suggested is assigning a security breach level indicating whether a breach of general information, confidential or proprietary information or loss in integrity of information.

Once the cause of the incident has been identified, the IT security breach incident response team should also document all known information including the attackers IP address, researching the host using incident databases and web searches.

The recovery process begins after the incident has been contained, eradicated and fully documented. The IT security team restores normal operation and validates functionality and performance of all systems. If necessary, backing up systems, disabling accounts or changing passwords, updating network security systems, equipment or hardware will be performed to prevent reoccurrence of the attack. Periodic follow-up should occur on a scheduled basis to ensure that the recovery solutions are still effective. Logs should be kept of all IT security incidents per the team's retention policy.

Following recovery, it's essential that a post-mortem or lessons learned session occur to dissect the causes of the incident, prevention and analyze the effectiveness of the eradication and recovery solutions implemented. If relevant and appropriate, any information deemed essential to the IT security breach risk mitigation plan should be included in it and updated as necessary.

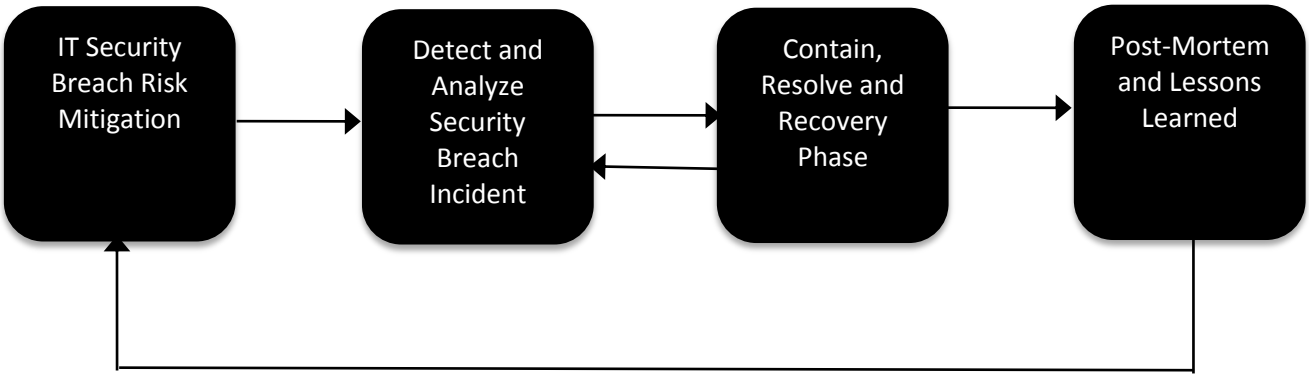

Figure 1: IT Security Breach Incident Response & Risk Mitigation (NIST)

6.6 Minimum Access Control Standards

Access of CFW network equipment defined in 6.4 should comply with Radio-008 and Appendix 1 of AR-D5 referenced in Section 8, which describes the City of Fort Worth Password Policy.

External Agencies should also enforce access control standards, functions and operating principles for network equipment utilized to connect to the CFW.

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 are also referenced in Section 8 of this policy.

6.7 External Agency Network Equipment Maintenance

Network Equipment that connects to the CFW radio system must comply with Radio-008 Network Maintenance Policy.

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.

6.8 Physical Security

Per AR-D5 section 10, the CFW recommends that external agencies also implement a physical security protection plan for building sites and IT assets from unauthorized access and disasters as well as restrict access to areas that house radio equipment utilized for connection to the P25 network.

Should a security breach occur that might impact the P25 network, the External Agency must immediately open an ITSM ticket via the Helpdesk procedure described in this document.

6.9 Network Perimeter Security

Requirements for External Connections

The following security structures are required per section 9.2.4.1 of AR-D5:

- External network connections to the CFW network will be via the perimeter securities managed point of entry only, which is the External Agencies Firewall/DMZ.
- Outbound services initiated from an internal address to an external address must be determined safe and approved via security assessment by the IT Security Manager.
- Inbound services initiated from an external address to an internal address must be determined safe and approved via security assessment by the IT Security Manager.
- External agencies connecting to the CFW network must sign an Interlocal Agreement before connectivity is established.

Security Equipment and Connectivity

External Agencies may only connect to the CFW network via the External Agency Firewall and DMZ (Demilitarized Zone) that resides at Eagle Mountain. The Firewall/DMZ is the CFW

perimeter security point of entry for all external connections whether through the Radio Network Interface (RNI) or Customer Enterprise Network (CEN).

External Agencies must provide their own Firewall/DMZ to protect their own networks and also the CFW network from unsecured networks. Firewalls must be Enterprise Grade, support Intrusion Prevention System (IPS) and be configured to be redundant in the event of a failure.

The information below outlines the specific requirements for external agencies with regards to security structures and points of entry on the CFW network:

- External Agencies requiring a Console or Network Management RNI level connection must access the CFW network via the External Agency Firewall/DMZ at Eagle Mountain.
- External Agencies utilizing Integrated Voice and Data (IV&D) functions specifically Over-the-Air Programming (OTAP) without a Presence Notifier (PN) will access the CFW network via the CEN. External Agencies with OTAP and a PN implemented on their own private networks will only require a PN to RNI level connection to the CFW network. In both cases the connection will occur via the External Agency Firewall/DMZ at Eagle Mountain.
- External Agencies implementing Over-the-Air-Rekeying (OTAR) without a Key Management Facility (KMF) Server will also connect via the CEN. If a KMF is utilized then a Border Router will be required to access the CFW network via the RNI. An agency specific Firewall is necessary. In both cases the connection will occur via the External Agency Firewall/DMZ at Eagle Mountain.
- External Agencies with NICE Logging equipment, specifically IP Loggers and AIS at their local dispatch centers must not directly connect to the CFW network. Agencies networks must be isolated from the RNI via an agency specific Firewall.
- External Agencies Consoles should only be loaded with Motorola software. 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 Consoles.

Network Connection Requirements

External Agencies connecting to the CFW radio network must ensure that their site links are dedicated circuits that meet Motorola performance specifications.

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

NIST Special Publication 800-61 Revision 2 August 2012
Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

CIS Center for Internet Security
https://msisac.cisecurity.org/members/local-government/documents/Cyber-Security-Risk-Management-for-Local-Governments.pdf

SANS Institute
https://www.sans.org/reading-room/analysts-program/breaches-happen

Title:	P25 Security Policy for External Customers	SOP No:	ITS-RADIO-007
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